ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Pojištění kybernetických rizik

Cyber risk insurance

Bc. Tereza Pacáková

Plzeň 2023

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma

„Pojištění kybernetických rizik“

vypracovala samostatně pod odborným dohledem vedoucí diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne 16. 4. 2023 v. r. *Bc. Tereza Pacáková*

Zásady pro vypracování práce

1. Vytvořte úvod do základní problematiky pojištění kybernetických rizik, definujte cíl a metodiku řešení.
2. Zpracujte teoretická východiska k problematice pojištění kybernetických rizik.
3. Na základě metody analýzy a komparace posuďte produktovou nabídku vybraných komerčních pojišťoven.
4. S využitím dotazníkového šetření objasněte chování obyvatel ČR v oblasti kybernetických rizik, shrňte jeho výsledky a zhodnoťte.
5. Shrňte řešenou problematiku a odhadněte možný budoucí vývoj.

Poděkování

Ráda bych poděkovala paní Ing. Janě Šturcové, Ph.D. za odborné vedení při psaní diplomové práce, za cenné rady a připomínky. Dále děkuji svojí sestře Kláře, která mi pomohla s jazykovou korekturou práce. V neposlední řadě, bych chtěla poděkovat paní Ing. Zdeňce Kováříkové, která mi poskytla materiály, které přispěly k vypracování diplomové práce.

Obsah

Úvod

Kvůli rozvoji online prostředí a moderních technologií jsou lidé stále častěji vystavováni kybernetickým hrozbám a rizikům. V IT systémech jsou ukládaná důvěrná data a citlivé údaje. Je zapotřebí tato data chránit a zabránit neoprávněným osobám k jejich přístupu. Kybernetickému útoku lze předcházet díky dodržování bezpečnostních opatření. Mezi ně patří například používání silných hesel nebo neukládání přihlašovacích údajů do internetových prohlížečů. Je důležité mít aktualizované antivirové programy a správně zabezpečenou informační síť. Dalším způsobem ochrany před kybernetickým hrozbami je pojištění kybernetických rizik. Účelem tohoto pojištění je pokrýt náklady vzniklé v důsledku kybernetického útoku.

Každým rokem narůstá počet provedených kybernetických útoků. Útoky začínají být sofistikovanější a hůře detekované. Mohou být cílené jak na jednotlivce, tak na společnosti. Na narůstající počty kybernetických útoků se společnosti snaží reagovat a přijímají různá opatření tak, aby předešly hackerskému útoku. Jedním ze způsobů, jak se bránit, je již zmíněné pojištění kybernetických rizik. Dále vznikají různé směrnice a vyhlášky, jejichž cílem je zvýšení zabezpečení proti kybernetickým hrozbám. Je důležité zvýšit povědomí o pojištění kybernetických rizik, aby společnosti i jednotlivci věděli, že se lze proti kybernetickým útokům chránit.

Diplomová práce bude rozdělená na část teoretickou a část praktickou. V první části budou rozebrána teoretická východiska ke kybernetickým rizikům. V praktické části bude analyzovaná produktová nabídka vybraných komerčních pojišťoven. Dále bude provedeno dotazníkové šetření zaměřené na chování obyvatel České republiky v oblasti kybernetických rizik.

Cíl a metodika

Hlavním cílem diplomové práce bude posouzení a zhodnocení produktové nabídky vybraných komerčních pojišťoven v oblasti pojištění kybernetických rizik. Dílčím cílem bude objasnit chování obyvatel České republiky v oblasti kybernetických rizik na základě dotazníkového šetření.

Teoretická část bude zpracována na základě teoretických pramenů, zákonů a vyhlášek, které mají souvislost s pojištěním kybernetických rizik. Jako základní literatura bude využita monografie od paní Evy Ducháčkové.

Praktická část bude zaměřená na rozbor a porovnání produktové nabídky vybraných komerčních pojišťoven pomocí metody analýzy a komparace. Dále bude zaměřená na dotazníkové šetření, které se bude zabývat chováním obyvatel České republiky v oblasti kybernetických rizik. Mezi vybrané pojišťovny patří Chubb, Colonnade, ČSOB, Maxima pojišťovna a Kooperativa. Analýza produktové nabídky pojišťoven bude provedena na základě všeobecných a zvláštních pojistných podmínek. Následně bude realizováno porovnání a zhodnocení produktové nabídky.

V lednu 2023 bude sestaven dotazník s celkem 15 otázkami. Dotazník bude rozdělen do dvou sekcí. První část bude zaměřená na identifikační údaje respondentů. Druhá část bude obsahovat otázky týkající se chování obyvatel v oblasti kybernetického pojištění. U dvou otázek bude využita funkce logické návaznosti. Dotazník bude vytvořen pomocí online dotazníkové nástroje Survio. Dotazníkové šetření bude zahájeno 1. února 2023 a bude ukončeno 10. března 2023. Během této doby odpovědělo celkem 341 respondentů. Návratnost dotazníků činila 96,1 %. Získaná data budou zhodnocena pomocí online nástroje Survio a tabulkového procesoru Excel.

1 Pojištění

Diplomová práce se bude zabývat pojištěním kybernetických rizik, proto je nutné nejprve vysvětlit základní pojmy, které s tímto tématem souvisí. Tyto pojmy budou vysvětleny v následujících podkapitolách.

V oblasti pojištění je typicky užívaným termínem nahodilá událost. Jedná se o událost, kterou nelze předvídat, očekávat nebo plánovat, dochází k ní náhle. Ekonomický subjekt má dvě možnosti, jak se s nastalou nahodilou událostí vyrovnat. Prvním způsobem je tzv. samopojištění neboli krytí z vlastních finančních zdrojů. Znamená to tvoření finanční rezervy, která bude v budoucnu krýt vzniklé nahodilé události. Negativem samopojištění je riziko, že naspořené peněžní prostředky nepokryjí vzniklou škodu. Další nevýhoda, která souvisí s touto možností, je vázanost finančních zdrojů do samopojištění. Peněžní prostředky by mohly být využity například na investování (Ducháčková, 2015).

Druhou možností, jak se lze vyrovnat s nahodilou událostí, je pojištění. V České republice je pojišťovací činnost upravena zákonem č. 277/2009 Sb. V § 3 je uvedena definice pojišťovací činnosti, která zní takto: „Pojišťovací činností je přebírání pojistných rizik na základě uzavřených pojistných smluv a plnění z nich. “ Dále je zde uvedeno, že s pojišťovací činností souvisí správa pojištění, likvidace škodných událostí, investování a poskytování asistenčních služeb (Zákony pro lidi, 2022).

Pojištění lze definovat jako finanční nástroj, který slouží k eliminaci negativních důsledků nahodilosti. Znamená to, že pomocí pojištění lze finančně uhradit ztráty, které vzniknou realizací čistých rizik (Ducháčková, 2009). Ministerstvo financí České republiky definuje pojištění jako přenesení negativních vlivů rizik tzv. škodných událostí na specializovanou osobu, tedy pojišťovnu. Škodné události mohou vést k újmě na majetku, zdraví nebo životě. Pojišťovna se za úplatu zavazuje poskytovat pojistná plnění v případě, že nastane nahodilá událost. Zjednodušeně lze konstatovat, že pojištění je finanční služba, jejímž hlavním cílem je tlumit finanční dopad nahodilých událostí. Pojištění chrání osoby před neočekávanými finančními výdaji a pomáhá předcházet platebním potížím (MONETA Money Bank, 2022a). Z ekonomického hlediska lze pojištění charakterizovat jako vytváření finančních rezerv z příspěvků zájemců o pojištění, které následně slouží pro krytí vzniklých škod.

Dle Ducháčkové (2015) lze pojištění vymezit pomocí následujících specifických znaků.

- **Pojištění je služba abstraktního charakteru** – pojišťovna se zavazuje k vyplacení přesně dané finanční náhrady, ale pouze v případě, když nastane definovaná nahodilá událost.
- **Nahodilost událostí** – nelze jednoznačně určit, zda příslušná událost nastane, není znám subjekt, který bude nahodilou událostí postižen a není zřejmý ani časový okamžik nastání události.
- **Pojištění je obvykle dlouhodobého charakteru.**
- **Typická je dopředu zaplacená úplata**.
- **Existence informační asymetrie –** účastníci pojištění mohou mít rozdílné informace.

1.1 Členění pojištění

Pojištění lze rozdělit podle různých hledisek. Jako první je v této podkapitole uvedeno členění dle právního hlediska. Podle toho hlediska rozlišujeme pojištění (Ducháčková, 2015):

- **dobrovolné** – sjednává se na základě pojistné smlouvy mezi pojišťovnou a zájemcem o pojištění na základně dobrovolného rozhodnutí.
- **povinné**
    - **povinné smluvní** – pojištění je dané právním předpisem, kdy je určena povinnost sjednání pojistné smlouvy pro dané subjekty. Příkladem toho typu pojištění je pojištění odpovědnosti z provozu vozidla.
    - **zákonné** – neuzavírá se pomocí pojistné smlouvy, ale je dáno zákonem a vzniká automaticky. Výše pojistného je přesně stanovena. Jedná se například o zdravotní pojištění v České republice.

Dle Ducháčkové (2015) lze dále rozdělit pojištění následovně.

- **Sociální pojištění –** patří do kategorie zákonného pojištění a je založeno na jiných principech než komerční pojištění. Ze sociálního pojištění jsou kryta rizika, která mají sociální charakter. Jedná se především o pracovní neschopnost, pracovní úrazy, potřeby zdravotní péče a potřeby v nezaměstnanosti. Toto pojištění nevzniká sepsáním smlouvy, ale je dané zákonem (Ducháčková, 2009).

- **Komerční pojištění (soukromé) -** vzniká na základě uzavření smlouvy mezi pojistníkem a pojistitelem, tedy pojišťovnou. Tento druh pojištění je založen na zásadě ekvivalence. To znamená, že velikost příspěvků od subjektů závisí na velikosti podstupovaného rizika. Komerční pojištění sjednávají komerční pojišťovny na základě dobrovolnosti a nabízejí subjektům různé druhy pojištění (Ducháčková, 2015).

Komerční pojištění lze dále rozdělit podle způsobu tvorby rezerv a dle druhu krytí pojistných nebezpečí. Dle způsobu tvorby rezerv rozlišujme:

- **pojištění riziková** – charakteristickým znakem rizikového pojištění je, že není jasné, zda vznikne pojistná událost a v jakém rozsahu. Platí zde podmíněná návratnost peněžních prostředků, která je daná vznikem pojistné události. V případě, že za celou pojistnou dobu nevznikne pojistná událost, pojišťovna nevyplácí plnění. V rámci sjednané doby pojištění může nastat neomezený počet událostí (Ducháčková, 2009). Tento druh pojištění nemá žádnou spořicí složku a placené pojistné je spotřebováváno na krytí pojistné ochrany a poplatky pojišťovny (MONETA Money Bank, 2022b).
- **pojištění rezervotvorná** – v tomto případě se tvoří rezerva na výplatu pojistného plnění v budoucnosti. Dalším rozdílem oproti rizikovému pojištění je fakt, že u rezervotvorného pojištění se pojistné plnění vyplácí téměř vždy.

Dle druhu krytí pojistných nebezpečí členíme na:

- **životní pojištění –** životní pojištění je určeno pro krytí rizika smrti nebo rizika dožití se určitého věku. V obou situacích bude vypláceno pojistné plnění. V případě smrti se bude plnění vyplácet osobám, které byly finančně závislé na příjmu zemřelého a nyní nemají prostředky k úhradě svých potřeb. Životní pojištění kryje životní události pojištěných (Ministerstvo financí Česká republika, 2014b).
- **neživotní pojištění** – kryje nebezpečí, která mají neživotní charakter. Neživotní pojištění lze dále rozdělit dle Ducháčkové (2015) na:
    - pojistná nebezpečí vztahující se k osobám – úrazové pojištění a nemocenské pojištění
    - majetková pojistná nebezpečí – pojištění domácností a nemovitostí, havarijní pojištění

- pojistná nebezpečí související s finančními ztrátami – úvěrová rizika, přerušení provozu
- pojistná nebezpečí spojená s odpovědností za škodu – občanská odpovědnost, pojištění odpovědnosti vůči zaměstnancům.

Dle Ducháčkové (2015) existují dvě formy pojištění. Obě dvě formy pojištění jsou upraveny novým občanským zákoníkem č. 89/2012 Sb. Konkrétně § 2821 upravuje obnosové pojištění a § 2811 škodové.

- **Obnosové pojištění –** někdy je nazýváno jako pojištění na pojistnou částku. U této formy pojištění bývá stanovena pojistná částka, která je shodná s pojistným plněním. Znamená to, že pojistné plnění je nezávislé na rozsahu vzniklé škody. Při vzniku pojistné události se vyplácí částka, která byla předem stanovena v pojistné smlouvě. U obnosového pojištění nelze přímo vyčíslit škodu. Jedná se především o pojištění zdraví, pojištění smrti, pojištění pracovní neschopnosti (Ducháčková, 2015).
- **Škodové pojištění** – pojistné plnění se odvíjí od výše nastalé škody. To znamená, že je vyplácena částka, která je buď nižší nebo rovna škodě. Škodové pojištění kryje konkrétní potřeby a jeho hlavním účelem je náhrada vzniklé škody. Za škodové pojištění lze označit pojištění domácnosti nebo pojištění nemovitosti (Ducháčková, 2009). U této formy pojištění se lze setkat s pojmy časová a nová cena. **Časová cena** je taková, kterou měla pojistná věc bezprostředně před vznikem pojistné události. Časová cena vychází z nové ceny, od které se buď odečítá znehodnocení a opotřebení pojištěné věci nebo, se naopak přičítá například modernizace. Za **novou cenu** lze v daném místě a čase koupit buď stejnou nebo podobnou věc shodného účelu. Lze si koupit ekvivalent pojištěné věci ve zcela nové a neopotřebené formě (Ducháčková, 2015).

1.2 Významné pojmy v pojišťovnictví

V této podkapitole budou objasněny významné pojmy, které souvisí s pojištěním a pojišťovnictvím. Budou zde představeny účastníci pojistného vztahu a pojmy jako pojistná smlouva, pojistné plnění, pojistná doba, pojistné podmínky.

Účastníci pojistného vztahu:

- **pojistitel** – „Právnická osoba, která je oprávněná provozovat pojišťovací činnost, tj. pojišťovna případně jiná instituce, které bylo uděleno povolení k provozování pojištění.“ (Česká asociace pojišťoven, 2022).
- **pojistník** – Jedná se o osobu fyzickou nebo právnickou, které uzavřela pojistnou smlouvu s pojistitelem. Pojistník je zavázán platit pojistné pojišťovně. Pojistník nemusí být pojištěným, sjednané pojištění je ve prospěch jiné osoby (ČSOB Pojišťovna, 2022a).
- **pojištěný** – „Pojištěným se rozumí osoba, na jejíž život, zdraví, majetek, odpovědnost za škodu nebo jiné hodnoty pojistného zájmu se soukromé pojištění vztahuje.“ (Česká asociace pojišťoven, 2022). Této osobě vzniká na základě pojistné smlouvy právo na výplatu pojistného plnění, bez ohledu na to, zda bylo pojištění sjednáno pojištěným nebo pojistníkem (Ducháčková, 2009).
- **obmyšlený** – „Osoba, určená pojistníkem, které vznikne právo na pojistné plnění v případě pojistné události, kterou je smrt pojištěného.“ (ČSOB Pojišťovna, 2022b). Obmyšlený může být uveden v pojistné smlouvě, určený zákonem nebo příbuzenským vztahem (ČSOB Pojišťovna, 2022b).
- **poškozený** – „Je osoba, která utrpěla škodu a uplatňuje nárok na její náhradu proti pojištěnému.“ (ČSOB Pojišťovna, 2022c). Typickým příkladem je pojištění odpovědnosti za škodu.

Definice **pojistné smlouvy** je uvedena v zákoně č. 89/2012 Sb. občanského zákoníku. § 2758 uvádí: „Pojistnou smlouvou se pojistitel zavazuje vůči pojistníkovi poskytnout jemu nebo třetí osobě pojistné plnění, nastane-li nahodilá událost krytá pojištěním (pojistná událost), a pojistník se zavazuje zaplatit pojistiteli pojistné.“ Jedná se o právní úkon, který vzniká mezi pojistitelem a pojistníkem, na základě toho úkonu vzniká smluvní pojištění právnických a fyzických osob. Pojistná smlouva musí být uzavřena v písemné podobě. Tato podmínka neplatí v případě, že je pojištění uzavíráno na dobu kratší než 1 rok (Ducháčková & Daňhel, 2010). Ve smlouvě by měly být uvedeny dle České bankovní asociace (2021) následující údaje:

- určení pojistitele a pojistníka, oprávněné osoby a jejich údaje,
- určení pojistné události,
- pojistné podmínky – vymezení vzniku a zániku pojištění, rozsah pojistného plnění, vymezení pojistné události,

- pojistná doba,
- pojistné – výše, splatnost, forma placení,
- forma pojištění,
- číslo smlouvy.

Pojistné je dopředu zaplacený finanční obnos za přenesení negativní důsledků nahodilé události na pojišťovnu. Je to finanční částka, kterou platí pojistník pojišťovně za poskytnutou pojistnou ochranu. Pojistné se hradí v předem dohodnutých časových intervalech.

Pojistné plnění je peněžní částka, která je vyplácená oprávněné osobě v důsledku vzniku pojistné událost. Pojistné plnění je vypláceno na základě podmínek, které jsou uvedené v pojistné smlouvě (Česká asociace pojišťoven, 2022). Pojišťovna zaplatí pojištěnému spravedlivou náhradu škody, které mu náleží na základě vzniku nahodilé události. Pojistné plnění bývá vypláceno pouze do výše skutečné škody (Ducháčková & Daňhel, 2012).

Pojistná doba je doba, na kterou je pojištění sjednáno. Tato doba je uvedena v pojistné smlouvě. Pojištění lze sjednat na dobu určitou nebo neurčitou. Na dobu určitou je stanoven konec splatnosti. Například stanovení pojistné doby na 10 let. Pojistnou dobu lze rozdělit na **pojistná období**. Pojistným obdobím rozumíme období, na které je hrazeno pojistné (Ducháčková, 2015).

2 Kybernetické riziko a kybernetický útok

V úvodu této kapitoly bude vysvětlen obecný pojem riziko. Následně již bude kapitola zaměřená na definování pojmů kybernetické riziko, kybernetický prostor a kybernetická bezpečnost.

2.1 Riziko

S pojištěním úzce souvisí pojem riziko, protože díky pojištění se před rizikem lze do jisté míry chránit. Existuje celá řada definic. Cipra (2015) definuje riziko jako „nebezpečí, možnost nepříznivých následků, vystavení ztrátě, nehodě či neštěstí." Ducháčková (2009) uvádí, že „riziko je chápáno jako možnost vzniku události s výsledkem odchylným od cíle s určitou objektivní pravděpodobností." U rizika lze vypočítat pravděpodobnost, se kterou může nastat. Řezáč (2011) uvádí mnoho různých definic rizika, jednou z nich je: „Riziko je pravděpodobnost, že se něco stane. Riziko je obvykle asociováno s nějakým negativním výsledkem, ačkoli jsou zde také možnosti pozitivní."

Na riziko se lze dívat z osobního nebo podnikatelského hlediska. Z osobního pohledu se za riziko považuje nemoc, ztráta blízkých nebo majetku. Zatímco podnikatelským rizikem je například ekonomická ztráta nebo úpadek společnosti. Dále lze rozeznávat různé druhy rizik. Pro účely diplomové práce bude uvedeno pouze pojistné riziko. Pojistné riziko se týká pojišťovací činnosti, která by měla poskytovat finanční ochranu před různými druhy nahodilých událostí (Cipra, 2015).

V závislosti na riziku mohou vzniknout buď negativní, nebo pozitivní odchylky od cíle. V případě negativní odchylky se jedná o čisté riziko, toto riziko není záměrně podstupované. Lze realizovat riziko, které bude mít záporné i kladné odchylky. Takové riziko je označováno jako riziko spekulativní. Znamená to, že lidé riziko podstupují zcela dobrovolně, jedná se například o investování, sázení nebo hazardní hry. Pojištění se věnuje pouze riziku čistému. Účelem pojištění je přesun rizika na pojistitele, který bude dané riziko finančně kompenzovat (Ducháčková 2015).

2.2 Kybernetické riziko

Pro vymezení pojmu kybernetické riziko je nutné nejprve definovat kybernetický prostor a kybernetickou hrozbu. Kybernetický prostor je digitální prostředí, které je celosvětově propojené a je tvořené informačními a počítačovými sítěmi, digitálními zařízeními,

systémy a procesy. Toto prostředí umožňuje výměnu, zpracování a vznik informací na celosvětové úrovni (zákon č. 181/2014 Sb.) Policie ČR (2022) definuje kyberprostor jako: „Virtuální prostředí, které nemá začátek a ani konec, nezná hranice národních států a nelze určit, jak rozsáhlé je.“ Kybernetický prostor není vlastněn žádnou osobou ani národem. Aktivity, které souvisejí s tímto prostorem, tak musí být komunikovány mezi všemi zúčastněnými stranami. Kybernetické prostředí lze vymezit podle následujících vlastností (Doucek a kol., 2019):

- **anonymita** – identita uživatele není známa,
- **asymetričnost** – aktivity jednoho uživatele mohou mít různý dopad na ostatní uživatele,
- **neexistence hranic,**
- **okamžitost** – jakákoli činnost v kybernetickém prostoru má okamžitý dopad,
- **volný vstup i ukončení pobytu v něm** – osoby mohou do prostoru volně vstupovat a vystupovat, neexistují žádné omezující podmínky,
- **interakce.**

V kybernetickém prostředí se nachází různé kybernetické hrozby. Kybernetická hrozba je negativní jev, který může mít různou závažnost a dochází k němu v digitálním prostředí. Jedná se například o spam, útoky na systémy, úniky informací a podobně (Ministerstvo vnitra České republiky, 2022).

Doucek a kol. (2019) definují kybernetické riziko jako: „Riziko způsobené kybernetickou hrozbou.“ Za kybernetické riziko lze považovat jakékoli riziko, které je spojené s finanční ztrátou, poškozením pověsti nebo únikem informací vyplývající ze zneužití informačních systémů společnosti (Northbridge Insurance, 2022). V současné době je pojem kybernetické riziko velmi aktuálním tématem. Dochází k rozvoji technologií a informačních sítí, je tedy více pravděpodobné, že bude přibývat kybernetických rizik a útoků. S využíváním nových moderních technologií roste také kybernetické riziko. Ducháčková (2015) ve své publikaci uvádí deset nejvýznamnějších podnikatelských rizik pro rok 2015. Kybernetický zločin a kybernetické riziko bylo na šestém místě. Dle Allianz barometru rizik pro rok 2022 je kybernetické riziko na prvním místě a stejně tomu bylo i v předcházejícím roce. Obdobná situace je například v Rakousku, Belgii nebo Německu. Je tedy patrné, že kybernetické riziko je celosvětově čím dál více rozšířené.

Kybernetické riziko lze rozdělit na interní a externí riziko. Interní riziko pochází zevnitř organizace a může být způsobeno úmyslně nebo neúmyslně. V případě, že se zaměstnanec společnosti rozhodne odcizit interní data, jedná se o úmyslné kybernetické riziko. Za neúmyslné riziko lze považovat špatnou instalaci bezpečnostního systému do sítě společnosti. Externí riziko pochází z vnějšího okolí organizace. Takovým rizikem je útok třetích stran nebo instalace viru do informační sítě (Sheth, 2020).

Dle průzkumu společnosti Deloitte je zaznamenán rostoucí trend spojený s kybernetickým rizikem. Největší nárůst byl registrován v době, kdy probíhala celosvětová pandemie covid – 19. V tomto období se většina činností přesunula do online prostředí, což přispělo ke zvýšenému kybernetickému riziku. Celkem 69 % dotázaných společností uvedlo, že v roce 2021 zaznamenaly nárůst kybernetických útoků. 87 % respondentů se chce v příštích letech více zaměřit na řízení kybernetického rizika a bezpečnosti (Deloitte, 2021).

2.3 Kybernetická bezpečnost

Hlavním cílem kybernetické bezpečnosti je ochrana všech zúčastněných stran v kybernetickém prostoru. Jedná se o ochranu v ekonomickém, politickém nebo vojenském oboru. Doucek a kol. (2019) uvádějí: „Kybernetická bezpečnost je souhrn právních, organizačních, technických a vzdělávacích prostředků, směřujících k zajištění ochrany kybernetického prostoru.“ K zajištění kybernetické bezpečnosti jsou prováděny různé aktivity, které mají za cíl udržet stabilní společnost, ochránit před riziky a zamezit následkům kybernetického rizika. Jsou to činnosti, které jsou potřebné k chránění informačních systémů a jejich uživatelů (Evropská rada, 2022a). V případě, kdy dojde k porušení kybernetické bezpečnosti, jedná se o kybernetický incident (útok).

Velká většina společností si stále myslí, že se jich kybernetická bezpečnost netýká. Jsou přesvědčené, že jejich interní data nemohou být odcizena a zneužita, že nejsou pro hackery tato data důležitá. Tímto přístupem ke kybernetické bezpečnosti se však vystavují vyšší pravděpodobnosti, že jejich společnost bude napadena (Arnold, 2017).

Kybernetická bezpečnost je velmi důležitá, hlavně v oblasti kritické infrastruktury. Je potřebné zajistit bezpečnost informačních a komunikačních technologií. Aby bylo předcházeno možným rizikům, vznikla regulace kybernetické bezpečnosti. V České republice byl vydán zákon, který tuto problematiku upravuje. Legislativní úprava bude

popsaná v podkapitole 4.2. Mezi hlavní důvody regulace kybernetické bezpečnosti patří (Doucek a kol., 2019):

- požadavky na úpravu kybernetické bezpečnosti ze strany celosvětových organizací – NATO, OSN, Evropská unie,
- neexistence hranic kybernetického prostoru – stanovení pravidel pro všechny zúčastněné osoby,
- rostoucí počty kybernetických útoků,
- investoři používají úroveň kybernetické bezpečnosti jako hodnotící kritérium,
- rychle se rozvíjející technologie a informační systémy,
- využívání různých technologií na každodenní bázi.

3 Kybernetické útoky

V této kapitole bude vysvětlen pojem kybernetický útok, bude uvedena definice útoku a dále průběh kybernetického útoku. V další části kapitoly budou útoky rozčleněny podle typu na útoky na fyzické osoby a na společnosti. Tyto typy budou detailně popsány a rozebrány.

Kybernetický útok je útok na informační a komunikační systémy s cílem způsobit škodu a získat citlivé a strategické informace. Realizované útoky mohou mít různé motivy, nejčastěji se jedná o politicky nebo vojensky motivovaný kybernetický útok (Jirásek a kol., 2013). Útok realizují takzvaní kyberzločinci, kteří pomocí svých počítačů napadají cizí sítě nebo počítače. Kyberzločinci mohou díky útokům například zcizit citlivá data, deaktivovat počítače, a to prostřednictvím malwaru, phishingu nebo ransomware. Útoky se mohou lišit podle toho, zda jsou provedeny začátečníkem, aktivistou, zločincem nebo interním útočníkem (Check Point, 2022). Útoky se skládají z několika následujících fází:

- průzkum a příprava,
- počáteční přístup,
- spouštění kódu,
- eskalace privilegií a perzistence,
- získání přístupových dat,
- šíření po síti a konečný cíl útoku.

Každá skupina zainteresovaná do kybernetického prostoru by se měla před kybernetickým útokem chránit. Prevencí jsou pravidelná školení o bezpečnosti na internetu, pravidelné aktualizace informačních a komunikačních systémů, ochrana e-mailů a správně zvolená přístupová hesla. Kybernetické útoky jsou čím dál více časté a nevyhýbají se ani České republice (Axians, 2022).

3.1 Útoky na fyzické osoby

Fyzické osoby nejsou kybernetickým útokům vystavovány tak často jako organizace a společnosti. Nejčastějším útokem, se kterým se fyzické osoby mohou setkat, jsou různé druhy podvodných e-mailů a zpráv, které chtějí z dané osoby vylákat peníze nebo získat její přístupové údaje do různých aplikací.

3.1.1 Malware

Slovo malware je složené z anglických slov malicious a software. V překladu malware znamená škodlivý software. Jedná se o program, jehož účelem je napadení systému tak, aby si toho uživatel nevšimnul. Cílem je získání nebo poškození dat, ovládnutí systému nebo dokonce sledování uživatele. Malware se do zařízení dostane pomocí zavirovaných webových stránek, stáhnutím her, programů, různých nástrojů nebo jakýchkoliv dat. Napadené zařízení lze poznat podle toho, že je zpomalené a velmi často dochází k pádu systému. Mezi druhy malwaru patří phishing, viry, trojské koně, počítačové červy, ransomware (Avast, 2022).

3.1.2 Podvodné e-maily a zprávy

Prvním druhem podvodného e-mailu nebo zprávy je vydávání se za určitou osobu nebo za osobu příbuznou. Tímto typem e-mailu nebo zprávy se osoby snaží vylákat z oběti peněžní prostředky. Typickým příkladem je vydávání se za vojáka, který je v Afganistánu a potřebuje zaslat peněžní prostředky na cestu domů. Důvěřivé osoby odešlou peníze, které však už nikdy neuvidí. Základním pravidlem a obranou je na tyto e-maily vůbec neodpovídat a rovnou je smazat z příchozí pošty, eventuálně vše nahlásit Policii ČR (Krausová, 2019). Tyto zprávy lze označovat názvem Nigerijské zprávy nebo také Nigerijský princ. Podvodné e-maily jsou také označované jako spam.

3.1.3 Phishing

Cílem phishingu je získání citlivých osobních informacích, přístupových údajů k internetovému bankovnictví, různých hesel, čísel karet a osobních účtů. Phishing se šíří pomocí podvodných e-mailů, které mohou buď odkazovat na falešné internetové stránky, nebo donutí příjemce zprávy stáhnout přílohy e-mailu (Avast, 2022). Phishingové e-maily napodobují e-maily od důvěryhodných společností, typickým příkladem jsou banky. V těchto e-mailech se vyskytuje odkaz na podvodné webové stránky a žádá uživatele o vyplnění přihlašovacích údajů. Podvodné webové stránky jsou k nerozeznání od pravých webových stránek. Ve chvíli, kdy jsou údaje na webové stránce vyplněny, data jsou hackerem odcizena a zneužita (Internetem bezpečně, 2022a). Phishingovým útokům lze předcházet pomocí následujících pravidel: neotvírat podezřelé e-maily ani jejich přílohy, neposílat citlivé údaje prostřednictvím e-mailu, kontrolovat podezřelé webové stránky a neklikat na žádné odkazy (ČSOB, 2022c).

3.1.4 Počítačový virus

Jedná se o ničivý program nebo programovací kód, který se šíří počítačem bez vědomí jeho uživatele. Počítačový virus se šíří kopírováním do různých dokumentů, které jsou v zařízení uložené. Dalším způsobem je kopírování do spustitelného programu. Hlavním cílem počítačového viru je napadení a získání kontroly nad počítačem nebo ukradení citlivých údajů. Když se virus dostane do počítače, provádí různé ničivé akce, jako je mazání uložených souborů v zařízení. Vir se dostane do počítače pomocí stažení zavirovaného souboru, stažení počítačové hry nebo díky zavirovanému USB disku (ESET, 2022).

3.1.5 Ransomware

Jedná se o druh malwaru, jehož cílem je uzamčení přístupu k zařízení nebo zašifrování uložených dat v systému. V případě, kdy je systém nakažen ransomware, je uživatel vydírán, aby zaplatil výkupné. Po zaplacení výkupného mají být zablokovaná data obnovena. Ani po zaplacení není jisté, že budou data zpřístupněna. Nejčastější způsob, jak se ransomware dostane do počítače je stažení příloh podezřelých e-mailů nebo otevření různých odkazů. Ochranou před tímto typem malwaru je mít všechna data zálohovaná. Zašifrovaná data se poté mohou smazat a ze systému se odstraní škodlivý vir (Internetem bezpečně, 2022b).

3.1.6 Počítačový červ

Počítačový červ je druh malwaru, jeho cíl je shodný s výše uvedenými útoky. Počítačoví červi se šíří pomocí sítě nebo přenosných médií. Účelem je nakazit virem co nejvíce zařízení. Nakažené zařízení lze poznat díky zpomalenému internetovému připojení, spotřebování velkého množství systémových prostředků nebo celkovému zpomalení zařízení. Počítačového červa si lze do zařízení stáhnout přílohou e-mailu nebo nakaženými webovými stránkami (Avast, 2022).

3.1.7 Spyware

Spyware je špehovací software, jehož cílem je sledování uživatele a tajné sbírání dat o něm. Hackeři sledují činnosti uživatelů na internetových stránkách, historii vyhledávání, zneužívají osobní údaje, jako je přístup k internetovému bankovnictví. Získané údaje jsou následně předávány třetím stranám. Uživatelé zařízení si nejčastěji

spyware stáhnou společně s jiným programem nebo otevřením přílohy e-mailu. Spyware je těžko odhalitelný a většina uživatelů si nevšimne, že je něco špatně. Nakažené zařízení lze poznat podle následujících znaků: antivirový program přestal fungovat, zpomalení počítače, změnilo se nastavení internetového prohlížeče, časté restartování systému nebo zaplnění paměti systému. Existují různé druhy spywaru, například keylogger zaznamenává vše, co bylo napsáno na počítačové klávesnici (Avast, 2022).

3.1.8 Ostatní druhy útoků

Výše byly zmíněné nejčastější druhy kybernetických útoků, existují však ještě další druhy. Jedná se například o trojského koně, adware, rootkit, vishing, krádež identity, internetový podvod nebo sociální inženýrství. Všechny útoky mají podobný cíl, snaží se o získání citlivých údajů, zablokování souborů v zařízení, vylákání peněžních prostředků nebo sběr dat o uživateli. Viry nebo nakažené kódy si většina uživatelů stáhne do zařízení pomocí příloh e-mailů, otevření podezřelých webových stránek nebo stažením programů (ESET, 2022).

3.2 Útoky na společnosti

Kybernetickým útokům čelí jak fyzické osoby, tak i společnosti. Firmy mohou být vystaveny všem výše zmíněným útokům a dále se setkávají s DDoS a APT útoky. Terčem kybernetických útoků jsou firmy po celém světě a nezáleží na druhu podnikání nebo velikosti společnosti. V současné době nejsou útokům vystavovány pouze velké firmy nebo veřejné instituce. Hackeři se zaměřili i na střední a malé podniky. Hlavním důvodem je fakt, že menší společnosti nebo podnikatelé mají slabou ochranu dat a počítačové sítě. Riziko kybernetického útoku se zvyšuje díky neustálému rozvoji IT technologií. K nárůstu útoků dále přispěla celosvětová pandemie covidu. V tomto období zaměstnanci hojně využívali home office a zabezpečení domácí IT sítě nebylo na takové úrovni jako ve firemním prostředí (RENOMIA, 2023a).

Mezi nejčastější následky kybernetického útoku dle Jirovského (2007) patří:

- **únik informací** – může se jednat o odcizení osobních údajů nebo dat z infomačního systému,
- **narušení integrity** – hackeři vymažou, změní nebo poškodí data společnosti,
- **potlačení služby** – díky kybernetickému útoku nebudou fungovat aplikace, systémy nebo webové stránky napadeného subjektu,

- **nelegitimní použití** – odcizená data a údaje budou použita neoprávněnými uživateli.

3.2.1 DDoS útok

DDoS je zkratka, která pochází z anglických slov „Distributed Denial of Service.“ Již z názvu je patrný cíl útočníků a provedení útoku. Hlavním cílem tohoto druhu útoku je odepření nebo znepřístupnění služby oprávněným uživatelům. Nejčastěji se jedná o znepřístupnění webových stránek, e-shopů nebo aplikací. Hackeři provádějí útok přes síť infikovaných počítačů z celého světa. Tato síť počítačů je označována jako distribuovaná botnet síť (ESET, 2023a).

DDoS útok funguje na principu přehlcení serveru požadavky. Síť infikovaných počítačů tzv. zombie odesílají velké množství požadavků, které daná služba nestíhá zpracovávat. Následkem útoku je zpomalení nebo úplně zastavení služby. Nevyžádané žádosti mohou být vysílané v řádu terabitů za sekundu. DDos útok lze poznat například tak, že se webové stránky dlouho načítají nebo se daná služba stane nedostupnou (Digitální pevnost, 2023).

DDoS útok lze tedy definovat jako: „Náhlý příliv umělého provozu navrženého tak, aby paralyzoval server webových stránek a učinil ho nepřístupným pro skutečné návštěvníky.“ (Schäferhoff, 2022). Znamená to, že server je zahlcen více požadavky, než je schopný zpracovat. Následkem je zpomalení nebo úplné selhání webu. Oprávněný uživatel tak není schopný načíst požadovanou stránku (Schäferhoff, 2022).

Existuje celá řada motivů, proč je tento typ útoku realizován. Jedná se především o následující důvody (Schäferhoff, 2022; ESET, 2023a):

- **finanční motiv** – hackeři mohou vydělávat na prodeji útoku jako služby nebo požadují výkupné za to, že přeruší DDoS útok,
- **hacktivismus** – jedná se o útok aktivistů, kteří nesouhlasí s rozhodnutím společnosti nebo reagují na nějaké kontroverzní prohlášení či politický ideál,
- **konkurenční boj** – cílem je získání konkurenční výhody na trhu, jedná se například o znepřístupnění webových stránek konkurenta během důležitého prodejního období,
- **poškození pověsti společnosti**,
- **prostředek k odvedení pozornosti** – DDoS útok slouží jako prostředek k odvedení pozornosti, aby zamaskoval jinou nekalou činnost.

3.2.2 APT útok

Název tohoto útoku pochází ze zkratky anglických slov „Advanced Persistent Threat“, což v překladu znamená pokročilé trvalé hrozby. V případě APT útoku se hacker dlouhodobě a nezákonně infiltruje do IT sítě. Účelem útoku je získání velmi citlivých dat. Jedná se především o obchodní tajemství, patenty a soukromá data zaměstnanců. Kyberzločinci mohou pomocí APT útoku také narušit kritickou organizační infrastrukturu nebo smazat databáze (Imperva, 2023).

Mezi hlavní charakteristiky APT útoku patří (AEC, 2023):

- **zaměření** – APT útoky jsou zaměřené na velké společnosti, finanční a vládní instituce, státy. Útok je vždy zaměřen na konkrétní cíl a je navržen specificky pro daný subjekt,
- **pokročilost** – pro infiltraci do systému se používají rootkity, techniky zatemnění a maskování,
- **perzistence** – APT útok přetrvává tak dlouho, dokud útočník nedosáhne svého záměru. Napadení systému trvá v některých případech až několik měsíců.

APT útok je rozdělen do čtyř následujících fází (Čermák, 2015; Hromada a kol., 2015).

- **Příprava –** v této fázi je snahou útočníka nashromáždit co nejvíce informací o subjektu, který se chystá napadnout. K vyhledávání informací využívá webové stránky, sociální sítě, diskuzní fóra. Dále zjišťuje, kdo za co v podniku odpovídá, jaké systémy a aplikace společnost používá a dále analyzuje stupeň zabezpečení. K výše zmíněným informacím se útočník zpravidla dostává pomocí sociálního inženýrství. Buduje si falešnou identitu, pomocí níž navazuje vztahy se zaměstnanci nebo se vydává za samotného zaměstnance. Poté dochází k přípravě samotného APT útoku, jedná se například o vývoj škodlivého malwaru a přípravu síťové infrastruktury.
- **Průnik –** ve fázi průniku dochází k šíření a spuštění škodlivého kódu, který byl vytvořen v přechozí fázi. Cílem je spustit tento kód na jednom nebo více zařízeních, které používají zaměstnanci pro vstup do systému. Existuje více způsobů, jak se do systému dostat. Jedním způsobem je technika, která se označuje jako watering hole. Znamená to, že útočník si v přípravné fázi zjistil, jaké internetové stránky zaměstnanci společnosti navštěvují nejčastěji. Následně

na tyto stránky umístí malware. Další metodou průniku jsou infikovaná paměťová média jako je CD nebo USB flash disk.

- **Kompromitace –** v této fázi je již firemní systém pod kontrolou útočníka, který hledá a sbírá citlivé informace a data. Dále vyhledává a napadá další systémy v IT síti společnosti.
- **Dokončení –** v této poslední fázi dochází ke kopírování dat, která byla získaná v přechozí fázi. Nemusí docházet pouze ke kopírování dat, útočníci mohou data smazat, zašifrovat nebo pozměnit. V některých případech dochází k vydírání postižené společnosti. Útočníci vyhrožují zveřejněním citlivých informací nebo prodejem dat konkurenci.

3.2.3 Review bombing

Hlavním smyslem tohoto typu útoku je poškození dobrého jména, služby, produktu nebo popularity podniku. Útok lze uskutečnit například i proti filmu nebo televizi. Za tento druh útoku je zodpovědný velký počet uživatelů nebo několik uživatelů, kteří vlastní více falešných účtů. Jejich hlavním cílem je zveřejnění co nejvíce negativních recenzí na daný produkt nebo službu. Většina zveřejněných recenzí je bez textu nebo se znění recenze opakuje stále dokola. Tato negativní hodnocení podávají ostatním uživatelům zkreslené informace o produktu a mohou je odradit od nákupu. Review bombing většinou realizují lidé, kteří například nesouhlasí s obsahem filmu nebo mají výhrady k jednání společnosti (Lye, 2022).

3.2.4 Blagging

V případě blaggingu je hlavním cílem získání finančního obnosu. Ve většině případů se k získání peněz využívá sociálního inženýrství. Podvodník se snaží o zmanipulování osoby prostřednictvím soucitu. Existují různé druhy blaggingu, ovšem záměr je ve všech případech stejný. Jedná se o vylákání peněz z oběti. Nejčastěji se podvodník vydává za osobu, kterou známe, může to být kamarád nebo rodina. Pod falešným účtem na sociálních sítích svou oběť kontaktuje s prosbou o finanční pomoc. Například uvede, že ztratil peněženku a požádá kamaráda o zaslání finanční obnosu. Tomuto typu blaggingu lze předcházet tím, že si ověříme profil na sociální síti nebo kontaktujeme kamaráda na jiných platformách a ověříme si jeho žádost o pomoc (Matějíček, 2021). Dalším způsobem blaggingu je vydávání se za ředitele firmy nebo partnera společnosti.

Podvodník kontaktuje zaměstnance firmy jako ředitel společnosti a požaduje zaplacení pohledávky nebo uzavření smlouvy. Podvodník musí mít dostatek informací o společnosti, aby mohl přesvědčit zaměstnance k provedení úkonu (Policie ČR, 2023).

EIOPA rozděluje kybernetické útoky dle frekvence výskytu, způsobených nákladů a podle následků. Z níže uvedené tabulky je patrné, že nejčastějším útokem je phishing, malware nebo ransomware a DDoS útok. Největší náklady vzniknout společnostem a organizacím, které jsou zasažené malware nebo DDoS útokem. Nákladná je především obnova dat a údajů. Za nejzávažnější následek útoku je považováno přerušení podnikání.

Tabulka 1: Rozdělení kybernetických útoků

FREKVENCE	NÁKLADY	NÁSLEDKY
Phishing	Malware, ransomware	Přerušení podnikání
Malware, ransomware	Phishing	Finanční náklady pro pojištěnce a třetí strany
DDoS	DDoS	Zničení dat a ztráta důvěry

Zdroj: EIOPA, 2019

3.3 Preventivní opatření proti kybernetickým útokům

Ze zprávy NÚKIB o stavu kybernetické bezpečnosti v roce 2021 je patrné, že kybernetické útoky jsou stále častější. V roce 2021 národní bezpečností tým České republiky řešil 1 726 bezpečnostních incidentů. V oblasti kybernetické kriminality a kriminality páchané na internetu bylo provedeno 9 518 trestných činů. V roce 2021 řešil NÚKIB celkem 157 incidentů, oproti roku 2020 se jedná o 59% nárůst, kdy bylo provedeno 99 útoků. Ze zprávy o kybernetické bezpečnosti lze vyčíst, že nejčastějším typem útoku byl DDoS útok, dále škodlivý kód jako je červ nebo spyware. Je patrné, že kybernetické útoky mají rostoucí trend, a proto je nezbytné se pro nim chránit a přijmout preventivní opatření. Tato opatření by se měla týkat jak jednotlivců, tak společností. Česká bankovní asociace přišla s tzv. Desaterem bezpečnosti, které má pomoci předcházet kybernetickým rizikům. Preventivní opatření a rady jsou následující:

- **bezpečnost počítače** – tato zásada se netýká pouze počítačů, ale je na místě mít správně zabezpečená všechna elektronická zařízení jako telefon nebo tablet. Ve všech zařízeních by měl být nainstalován aktuální antivir a firewall. Díky

aktualizované antivirové ochraně lze předejít kybernetickým útokům. Oproti předchozím letům jsou v dnešní době antivirové programy schopny chránit zařízení před malwarem, ransomwarem, phishingem nebo před škodlivými aplikacemi. Je důležité mít nainstalovaný antivir i v mobilním zařízení. Uživatelé si mohou do telefonu stáhnout škodlivou aplikaci, která následně odcizuje přihlašovací údaje do bankovnictví (ESET, 2023b).

- **zabezpečení telefonu** – platbu mobilním telefonem využívá stále více lidí. Při bezkontaktním placení telefonem je důležité používat správné zabezpečení telefonu. Za nejbezpečnější způsob je považováno biometrické ověření. Uživatelé mohou používat k odemčení telefonu buď otisk prstu nebo scan obličeje. Pomocí biometrických údajů lze potvrzovat i online platby. Mezi další druhy zabezpečení patří PIN kód, znak a heslo. Za nejméně bezpečný způsob je považováno odemykání telefonu pomocí znaku, je totiž snadno prolomitelný. Heslo je bezpečné v případě, že je dostatečně silné. Nejlepší ochranou telefonu je využití dvojitého zabezpečení. Jedná se například o kombinaci biometrických údajů a PIN kódu (Digitální pevnost, 2019).
- **ochrana přihlašovacích údajů** – je důležité chránit všechny přihlašovací údaje, včetně těch k internetovému bankovnictví. Přihlašovací údaje jsou citlivé informace, které by neměly být sdělovány jiným osobám. Dále je důležité údaje neukládat v počítači nebo telefonu (Česká bankovní asociace, 2023).
- **PIN –** nejčastěji se jedná o čtyřmístný kód, který slouží jako ověření při platbě kartou. Tento kód by měl být pro uživatele snadno zapamatovatelný nikoli však snadno odhadnutelný. Za nevhodnou kombinaci čísel se považuje datum narození, telefonní číslo nebo posloupnost čísel typu 1234. PIN není vhodné nikomu sdělovat. Pokud si uživatel musí PIN zapsat, není vhodné, aby byl kód uložený v blízkosti platební karty (Česká spořitelna, 2023).
- **bezpečné heslo –** bezpečné heslo je takové, které je silné, neodhadnutelné, nezjistitelné, dostatečně dlouhé a unikátní. Není vhodné volit hesla, která obsahují jména rodiny nebo mazlíčků, slova ze slovníků, číselnou posloupnost nebo heslo typu password. Bezpečné heslo by mělo být dlouhé minimálně 8 znaků a mělo by obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků. Heslo by mělo být také unikátní. To znamená, že uživatel zvolí jiné heslo pro internetové bankovnictví a odlišné pro sociální sítě. Jak již bylo zmíněno výše, hesla nemají

být nikomu sdělována a ukládána do internetových prohlížečů (Česká bankovní asociace, 2023).

- **podezřelé přílohy –** důležitou prevencí proti kybernetickému útoku je kontrola příchozích e-mailů a následně i příloh. Je doporučeno e-maily od podezřelých odesílatelů vůbec neotvírat, nestahovat žádné přílohy ani neklikat na žádné odkazy, které v e-mailu přišly. V případě, že se jedná o spam nebo phishing, text e-mailu obsahuje gramatické a stylistické chyby. Dále je nutné zkontrolovat adresu odesílatele, zda neobsahuje jiné znaky. Například moneybank.cz lze zaměnit za rnoneybank.cz. Na první pohled nemusí být patrné, že druhá adresa není správná. Místo písmene „m“ jsou zde uvedena písmena „r“ a „n“. Do takto podezřelých e-mailů není vhodné zadávat žádné osobní údaje nebo přihlašovací údaje (Kohout, 2018).
- **správně zabezpečená IT síť –** bezpečnost sítě se kontroluje v různých oblastech například: řízení přístupu zaměstnanců, ochrana zpracovávaných informací, reakce na bezpečnostní hrozby nebo bezpečnost při spolupráci s externími subjekty (ESET, 2023c).
- **školení zaměstnanců –** lidská chyba patří mezi časté příčiny vzniku kybernetických rizik, a proto je nutné zaměstnance proškolovat v oblasti kybernetických rizik. Zaměstnance lze proškolit v oblasti práce s informacemi, vytváření bezpečných hesel, rozpoznávání hrozeb, používání webu nebo používání datových úložišť.
- **znalost problematiky kybernetických útoků –** jedná se o znalost kybernetické bezpečnosti, jaká jsou rizika a dopady kybernetických útoků, jak útok identifikovat, jak se správné zabezpečit nebo jak bezpečně používat digitální technologie (Bezpečnost práce, 2022).

4 Pojištění kybernetických rizik

Tato kapitola se bude zabývat historií a legislativou pojištění kybernetických rizik. Bude zde vysvětleno, co je pojištění kybernetických rizik a jaká rizika lze pojistit. V kapitole budou uvedeny hlavní příčiny vzniku kybernetických rizik a jejich dopady. Kapitola bude dále obsahovat porovnání výhod a nevýhod tohoto pojištění a proč je důležité se pojistit proti kybernetickým rizikům.

4.1 Definice

Kybernetická rizika jsou součástí každodenního života a jsou jim vystavovány osoby a společnosti, které přichází do kontaktu s elektronickými daty. Rizika mohou být různá, jedná se o ztrátu počítače, neoprávněný zásah do systému nebo přerušení webových služeb. Dle společnosti RENOMIA jsou kybernetickému riziku vystavovány především podniky, které:

- zpracovávají velké množství klientských, osobních nebo zaměstnaneckých dat,
- využívají aktivně sociální sítě a webové stránky,
- akceptují platby kartou nebo využívají elektronických plateb,
- ukládají data na externí úložiště,
- svojí podnikatelskou činností závisí na online IT řešeních.

Pojištění kybernetických rizik patří do kategorie škodových neživotních pojištění. Jedná se o kombinaci pojištění odpovědnosti za finanční škody vůči třetím stranám a finanční škody způsobené přímo pojištěnému. V rámci pojištění kybernetických rizik nejsou kryty hmotné škody na majetku a újmy na zdraví. Oběť incidentu (viník) obvykle musí uhradit poškozeným třetím stranám ušlý zisk a náklady na obnovu dat a systémů. Pojištěnému mohou kvůli kybernetickému útoku vzniknout následující finanční výdaje (RENOMIA, 2023b):

- náklady na mimořádnou událost – např. najmutí IT znalce,
- náklady na obnovu dat a systémů,
- náklady na právní zastoupení,
- ušlý zisk kvůli přerušení provozu,
- náklady na regulatorní řízení,
- sankce za únik údajů (GDPR).

Výše pojistného a pojistné podmínky se stanovují individuálně podle potřeb zájemců o pojištění. Důležitým faktorem pro stanovení pojištění je obor podnikatelské činnosti a množství zpracovávaných údajů. Mezi další rozhodující činitele patří způsob ochrany dat společnosti, požadované limity pojistného plnění, požadované krytí a také rozsah outsourcingových služeb. Pojištění kryje různá rizika v závislosti na tom, jaké konkrétní pojištění si klienti sjednají. Lze se pojistit proti následujícím hrozbám (RENOMIA, 2023a):

- poškození dobrého jména,
- ztráta zisku z důvodu přerušení provozu,
- udělení pokuty od Úřadu pro ochranu osobních údajů,
- vydírání prostřednictvím IT sítě
- odpovědnost společnosti za důvěrná data zaměstnanců, klientů, partnerů,
- narušení ochrany dat,
- obnova dat.

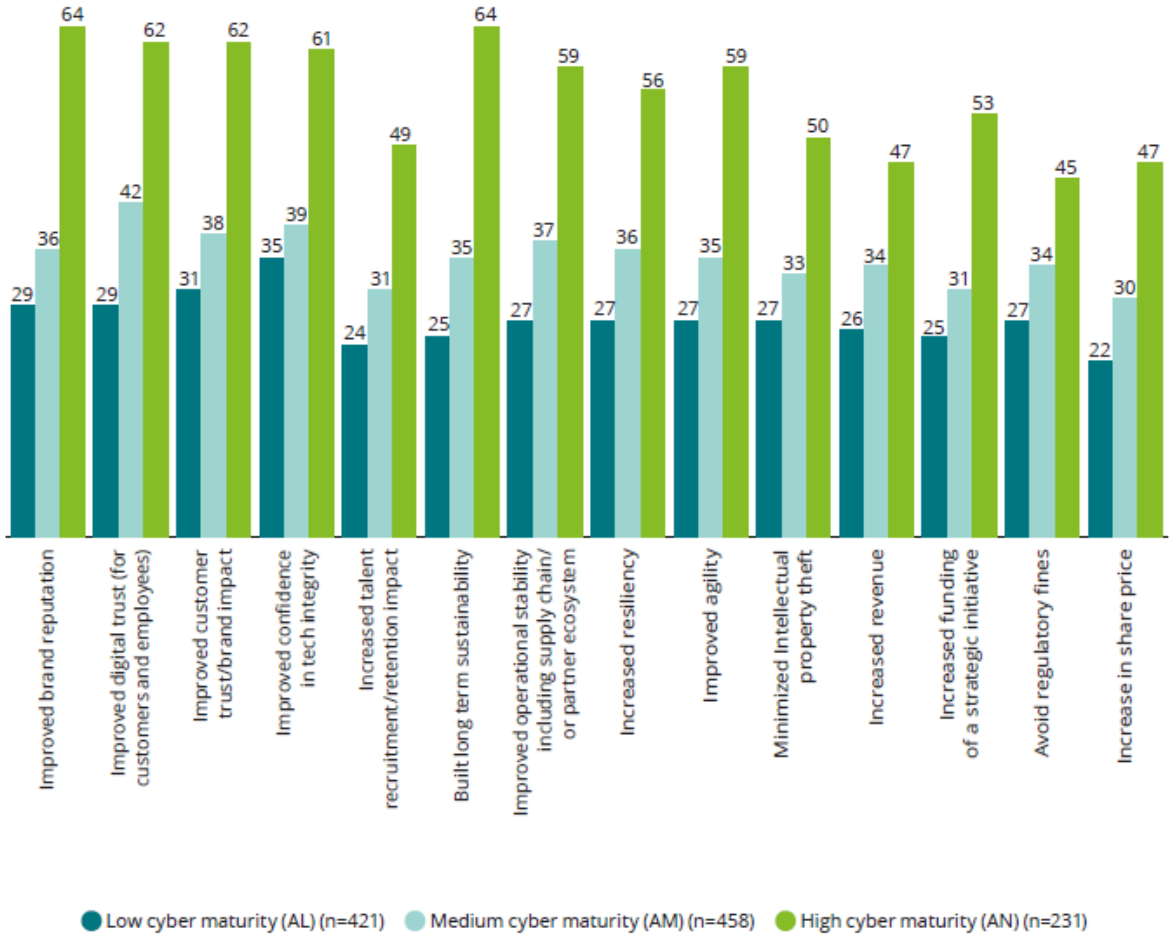
Mezi hlavní příčiny vzniku kybernetických incidentů patří podle společnosti RENOMIA následující možnosti:

- **lidský faktor** – jedná se o zaměstnance, kteří kvůli nedbalosti umožnili kybernetický útok. Například připojili do počítačové sítě společnosti neověřené externí zařízení. Někteří pracovníci mohou jednat i úmyslně s cílem poškodit zaměstnavatele.
- **technologie** – v tomto případě je hlavním problémem zastaralý hardware a software, neaktualizované antivirové systémy a nedostatečná ochrana dat.
- **ztráta/zcizení hardwaru** – společnosti mohou být odcizena přenosná zařízení, která obsahují důvěrná data.
- **hackerský útok** – podnik je vystaven některému z rizik, které jsou uvedená v kapitole 3.

Je patrné, že kybernetických útoků každým rokem přibývá, a proto je důležité, aby společnosti a podniky využívaly pojištění kybernetického rizika. Díky tomuto pojištění jsou chráněny proti škodám, které vznikly v důsledku útoku. Z pojištění jsou kryty náklady a finanční ztráty, ušlý zisk, odborníci a také sankce a pokuty. Nevýhodou tohoto druhu pojištění je vyplnění vstupního dotazníku. Tento dotazník je poměrně dlouhý a detailně zkoumá IT zabezpečení klienta a nakládání s daty.

Společnost Deloitte prováděla průzkum, který se týkal řízení kybernetických rizik a budoucnosti kybernetiky. Průzkum ukázal, že společnosti se v současné době mnohem více zabývají kybernetickým rizikem. 70 % dotázaných uvedlo, že se vedení společnosti zabývá řízením kybernetických rizik alespoň jednou za měsíc nebo jednou za čtvrt roku. Z výzkumu vyplynulo, že společnosti, které se zabývají řízením kybernetických rizik, pociťují různé pozitivní přínosy. Jedná se například o zvýšení obratu, zlepšení pověsti značky, zlepšení důvěry zákazníků, lepší stabilitu dodavatelského řetězce nebo vyhnutí se regulačním poplatkům. Všechny pozitivní přínosy jsou uvedené na následujícím grafu.

Obrázek 1: Pozitivní přínosy řízení kybernetických rizik



Zdroj: Deloitte, 2023

4.2 Legislativa

Pojišťovnictví je upraveno zákonem č. 277/2009 Sb. o pojišťovnictví. V tomto zákoně lze nalézt definici pojišťovací činnosti. Dále jsou zde uvedeny podmínky provozování činnosti v pojišťovnictví. V zákoně jsou vysvětleny pojmy, které s pojišťovnictvím souvisí, například definice pojišťovny a její základní kapitál.

Další legislativní úprava je obsažena v novém občanském zákoníku č. 89/2012 Sb. Zde jsou vysvětleny pojmy jako pojistná smlouva, obnosové a škodové pojištění, pojištěný, pojistka, povinné pojištění a také zánik pojištění.

Kybernetická bezpečnost je v České republice upravena následující legislativou:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti,
- GDPR,
- směrnice NIS, NIS 2,
- DORA,
- ISO normy 27000, 27100, 27101, 27103.

Zákon o kybernetické bezpečnosti vstoupil v účinnost 1. ledna 2015 a upravuje práva a povinnosti osob, dále pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon definuje základní pojmy jako je kybernetický prostor, kybernetická bezpečnost, významné informační systémy a správce informačních a komunikačních systémů. Mezi hlavní cíle zákona patří stanovení bezpečnostních opatření, zlepšení detekce kybernetických incidentů, zavedení hlášení o kybernetických incidentech a zavedení systému opatření k reakci na bezpečnostní incidenty. Zákon o kybernetické bezpečnosti zpracovává příslušné směrnice Evropské unie, konkrétně směrnici NIS (NÚKIB, 2023).

Zákon dále ukládá povinnost orgánům a osobám uvedeným v § 3 tohoto zákona bezodkladně hlásit kybernetické útoky a incidenty. Subjekty, které zajišťují významnou síť nebo jsou poskytovatelem digitálních služeb hlásí incidenty národnímu CERT. Ostatní orgány a osoby hlásí bezpečnostní incidenty vládnímu CERT. Hlášení by mělo obsahovat typ incidentu, údaje o systému, kde se kybernetický útok vyskytl, údaje o zdroji incidentu a dále jakým způsobem byl útok řešen a výsledky řešení. V závislosti na tom, o jaký bezpečnostní incident se jedná, mohou být vydána následující opatření: varování,

reaktivní opatření a ochranné opatření. Varování zveřejňuje vládní CERT na svých internetových stránkách a dále varování rozesílá povinným osobám. Tento typ opatření je pouze informativního charakteru. Účelem reaktivního opatření je provést opatření k řešení kybernetického incidentu a zabezpečení informačních systémů a sítí. Posledním typem opatření je ochranné opatření, které je velmi podobné reaktivnímu, má spíše preventivní charakter a je obecnější (zákon č. 181/2014 Sb.).

Vyhláška č. 82/2018 Sb. je vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Navazuje na zákon o kybernetické bezpečnosti a také na směrnice Evropské unie. Vyhláška upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- rozsah a obsah bezpečnostních opatření,
- metody a náležitosti hlášení incidentu,
- hodnocení významnosti kybernetických incidentů,
- způsob likvidace dat,
- informace o provedení opatření.

Vyhláška dále definuje organizační bezpečnost, řízení rizik, řízení dodavatelů, bezpečnost lidských zdrojů, zvládání kybernetických bezpečnostních incidentů nebo audit kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.).

V České republice platil zákon č. 101/2000 Sb. o ochraně osobních údajů. Tento zákon byl v roce 2018 nahrazen **Obecným nařízením o ochraně osobních údajů** (GDPR). Celý název je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Ministerstvo vnitra České republiky, 2023). Jedná se o obecné nařízení, které stanovuje pravidla pro zpracovávání osobních údajů a práv subjektu údajů. Toto nařízení je univerzální a platí ve všech státech Evropské unie. Cílem GDPR bylo sjednocení právního rámce ochrany osobních údajů. Obecné nařízení hájí práva občanů, aby jejich osobní údaje a data nebyla neoprávněně používána. Toto nařízení o ochraně osobních údajů definuje základní práva fyzických osob v digitálním světě, povinnosti zpracovatelů údajů, metody zajištění souladu a sankce pro osoby, které porušují pravidla. Díky GDPR je chráněno soukromí a data spotřebitelů jsou bezpečně zpracovávána (Evropská rada, 2023).

Směrnice NIS neboli Network Information Security je směrnice Evropské unie, jejímž cílem je zajištění vysoké míry bezpečnosti informačních systémů a sítí. Hlavním účelem směrnice je sjednocení právní úpravy členských států EU v oblasti kybernetické bezpečnosti. Členské státy měly povinnost tuto směrnici implementovat do svých národních právních úprav. Česká republika již v této době měla zákon o kybernetické bezpečnosti, proto stačilo zákon pouze novelizovat o povinnosti stanovené NIS. Směrnice vstoupila v platnost v roce 2016 a stanovila následující požadavky (Duračinská, 2016):

- přijetí strategie – členské státy mají povinnost přijmout strategii pro bezpečnost sítí a infomačních systémů,
- zřízení centrálního orgánu – zřízení národního orgánu pro řízení kybernetické bezpečnosti,
- zřízení CSIRT týmu – jedná se o skupinu, která reaguje na incidenty v oblasti počítačové bezpečnosti. Zajišťuje základní služby a provozuje elektronické služby.

V prosinci roku 2022 byla přijata nová směrnice Evropské unie **NIS 2**. Tato nová směrnice nahrazuje původní NIS a jedná se o její rozšíření a prohloubení v oblasti kybernetické bezpečnosti. Hlavním cílem je zajištění vysoké úrovně kybernetické bezpečnosti, zlepšení odolnosti veřejného a soukromého sektoru a schopnost správně reagovat na bezpečnostní incidenty. Nová směrnice obsahuje následující změny (Evropská rada, 2022b):

- **zřízení evropské sítě styčných organizací** – tyto organizace se budou zabývat řešením rozsáhlých kybernetických útoků a incidentů,
- **nápravná opatření a sankce,**
- **aktualizace seznamu odvětví a činností na něž se směrnice vztahuje**,
- **pravidlo velikostního omezení** – nově se budou směrnicí řídit střední a velké organizace, které jsou uvedené v seznamech odvětví a činností,
- **vyšší úroveň řízení rizik,**
- **zjednodušení povinného hlášení o kybernetických incidentech,**
- **soulad s právními předpisy DORA a CER**.

DORA je nařízení Evropské komise o digitální provozní odolnosti. Cílem tohoto nařízení je snížení rizik, která souvisí s užíváním informačních technologií, a zvýšení odolnosti finančního systému. Toho bude dosahováno pomocí pravidel, která budou platná v celé

Evropské unii. DORA se týká především finančního sektoru, pro který jsou zavedena regulatorní a dohledová opatření. Tyto standardy budou muset dodržovat banky, úvěrové instituce, pojišťovny, obchodníci s cennými papíry a také třetí strany, které zajišťují pro finanční sektor kritické služby týkající se informačních a komunikačních technologií. Na základě nařízení o digitální provozní odolnosti musí všechny organizace, kterých se to týká, zajistit, že jsou schopné přestát kybernetických incident, reagovat na hrozbu a poté se z ní zotavit. Jak uvádí pan Plecháček v časopise Bankovnictví klíčem k silné kybernetické bezpečnosti je nepřetržitý monitoring, identifikace rizik a automatizované ověřování efektivity bezpečnostních technologií a týmů. DORA vstoupila v platnost 16. ledna 2023 (Plecháček & Dudková, 2022).

Kybernetickou bezpečnost dále upravují různé **ISO normy**. V normě ISO 27100 jsou definovány pojmy kybernetický prostor, kybernetická hrozba a kybernetické riziko. V normě 27000 jsou uvedeny základní pojmy, které se týkají bezpečnosti informací, například integrita, bezpečnostní funkce nebo bezpečnost informací (Doucek a kol., 2019).

4.3 Historie

V 90. letech 20. století došlo v USA k rozvoji internetu a počítačové technologie. S tímto rozvojem začaly vznikat první kybernetické hrozby a incidenty. Jednalo se především o neoprávněný přístup do systémů, počítačové viry a únik dat. Zpočátku se pojištění kybernetických rizik vztahovalo pouze na chyby při zpracování dat. Později se začal pojistný trh s pojištěním kybernetických hrozeb rozvíjet. Pojištění se vztahovalo na kybernetická rizika jako je počítačový vir, ztráta dat a neoprávněný přístup do systému. Kybernetické pojištění bylo původně součástí pojištění odpovědnosti a vztahovalo se pouze na organizace, které působily v profesionálních službách a technologiích. Produkty kybernetického pojištění se zprvu vztahovaly pouze na pokrytí závazků třetích stran. V roce 2000 došlo ke změně a pojištění se začalo vztahovat i na samotné oběti kybernetického útoku, jednalo se například o krytí ušlého zisku (ColonyWest, 2023).

V roce 2003 byl v Kalifornii přijat zákon, který se týkal kybernetické bezpečnosti. Účelem toho zákona bylo informovat osoby, jejichž data byla zneužita nebo odcizena. Po vzoru Kalifornie začaly i ostatní státy přijímat různá nařízení a zákony, které se zabývaly kybernetickou bezpečností. V tomto období došlo k nárůstu kybernetických útoků a incidentů, což vedlo také k růstu zájmu o pojištění kybernetických rizik. Pojištění je tak

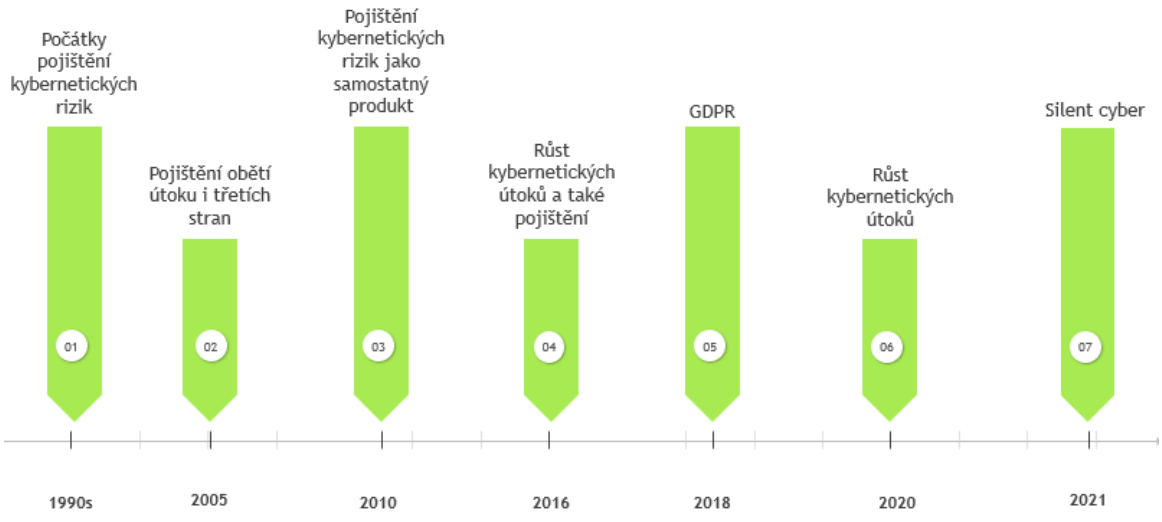
častěji nabízeno jako samostatný pojistný produkt a ne jako součást pojištění odpovědnosti.

Postupně dochází k rozvoji sofistikovanějších kybernetických hrozeb a útoků na veškeré organizace. Proto je potřeba zavést pojistný produkt, který nebude určen pouze pro některé obory nebo odvětví. Roste tedy opět poptávka po pojištění kybernetických rizik. V roce 2018 vstoupila v platnost nařízení Evropské unie o ochraně dat neboli GDPR.

V roce 2020 svět zasáhla pandemie covid-19, která měla velký vliv na pojištění kybernetických rizik. V době pandemie byly společnosti nuceny zavádět tzv. home office. To způsobilo nárůst používání mobilních zařízení a dále vzdáleného přístupu do podnikových systémů. Zabezpečení nebylo na vysoké úrovni, čehož využili kyberzločinci a narostl počet kybernetických incidentů. Pandemie tak přispěla k rozvoji pojištění kybernetických rizik, protože se ukázalo, že je velmi potřebné a žádoucí (Morris, 2021).

Od roku 2021 se musejí společnosti i fyzické osoby vyrovnávat s tzv. „silent cyber“. Jedná se o „tiché“ kybernetické útoky. Například útočníci pronikli do ovládacího systému vlaku, který následně vykolejil, nebo pomocí malwaru pronikli do navigačního systému a díky tomu navedli loď na útes. V důsledku toho vznikají fyzické škody (Allianz, 2023).

Obrázek 2: Historie pojištění kybernetických rizik



Zdroj: Vlastní zpracování dle Morris, 2023

5 Produktová nabídka vybraných pojišťoven

Cílem této kapitoly bude na základě metody analýzy a komparace posoudit produktovou nabídku vybraných pojišťoven. Analyzovaným produktem bude pojištění kybernetických rizik. V kapitole budou zmapovány pojistné podmínky, předměty pojištění, omezení v pojistném krytí a také výluky v pojištění. Následně bude provedeno porovnání nabízených pojistných produktů.

V současné době není pojištění kybernetických rizik na pojistném trhu příliš rozšířené. Pojištění kybernetických rizik v České republice nabízí celkem pět pojišťoven. Jedná se o následující pojišťovny: Chubb, Colonnade, ČSOB, Kooperativa a Maxima pojišťovna. Některé pojišťovny nabízejí přímo produkt pojištění kybernetických rizik, jiné mají tento typ pojištění zahrnut v rámci jiných pojistných produktů. V tomto případě se většinou jedná o pojištění internetových rizik a je určené především pro jednotlivce. Pojištění internetových rizik bývá součástí pojištění domácností. Pojištění kybernetických rizik jako takové je zaměřené spíše na společnosti a organizace.

Jak uvádí časopis Pojistný obzor (2018): „Kybernetické pojištění je jedním ze způsobů přenosu rizika spojeného se vznikem finančních nákladů způsobených kybernetickým útokem a zároveň se jím zajišťuje asistence postiženým.“ Pojištění kybernetických rizik z veřejnoprávního hlediska spadá do kategorie neživotního pojištění. Z pohledu soukromoprávního lze toto pojištění zařadit do škodových pojištění. Klíčové je pro tento pojistný produkt správné posouzení a vyhodnocení kybernetických rizik. V současné době je to prováděno pomocí nástrojů monitorování a dále pomocí dotazníků kybernetických rizik.

V následujících podkapitolách budou uvedeny pojistné produkty od výše zmíněných pěti pojišťoven. U každého pojistného produktu bude uvedeno, na jaká rizika se pojištění vztahuje a jaké kryje náklady. Budou zde také uvedeny výluky, na které se pojištění kybernetických rizik nevztahuje. Produktová nabídka vybraných pojišťoven byla zpracována na základě jednotlivých všeobecných a zvláštních pojistných podmínek a dále dle interního materiálu společnosti RENOMIA. Na závěr kapitoly bude uvedena tabulka, která bude podávat přehled o srovnání pojištění kybernetických rizik.

5.1 Chubb pojišťovna

Chubb pojišťovna svým klientům nabízí pojištění kybernetických rizik, které se nazývá Cyber Enterprise Risk Management. Pojistné podmínky lze rozdělit na dvě části, a to na rozsah pojištění a výluky, které pojištění nekryje. Prvním rizikem je **neoprávněné nakládání s údaji**. Tím se rozumí skutečné nebo údajné jednání nebo chyba, které se pojištěný dopustil při shromažďování, uchovávání, či jiném zpracování dat. Jedná se především o osobní data a data třetích stran, která byla označena za důvěrná. Pojištění se nevztahuje na škody, které souvisejí s patentem nebo obchodním tajemstvím. Pojištění kryje i odpovědnost za data v papírové podobě.

Kybernetické pojištění dále kryje **odpovědnost za narušení bezpečnosti sítě**. Za narušení sítě se považuje zavedení malwaru, zásah hackera, DDoS útok a neoprávněné užití či přístup. Pojištění se vztahuje i na **odpovědnost za zpřístupnění dat třetí osobě zaměstnancem**. Pojištění se týká také **odpovědnosti v souvislosti s médii**. Mediálním obsahem se rozumí elektronický obsah šířený na internetu pojištěným nebo jménem pojištěného, včetně jeho šíření prostřednictvím sociálních sítí. Za protiprávní jednání dle pojistných podmínek lze považovat: poškození pověsti, pomluvu, urážku, odposlech, plagiátorství, počítačové pirátství.

Další oblast, kterou pojištění Cyber Enterprise Risk Management kryje je **kybernetické vydírání**. Pojišťovna Chubb dle svých pojistných podmínek považuje za kybernetické vydírání hrozbu, pomocí které třetí strana pojištěnému oznamuje následující záměry:

- zveřejnění, zpřístupnění, zničení dat uložených v systému pojištěného,
- poškození, zničení, smazání dat a elektronických informací,
- zavedení malwaru,
- znepřístupnění počítačového systému,
- zahájení útoku na počítačový systém pojištěného.

Předposledním rizikem, které je uvedeno v pojistných podmínkách je **ztráta a narušení dat.** Ztrátou či narušením dat se rozumí přístup k datům pojištěného, jejich ztráta, zničení nebo poškození. Data lze poškodit neoprávněným elektronickým zásahem, malwarem, zásahem hackera, DDoS útokem, lidskou chybou nebo chybou programu. **Přerušení provozu** je narušení počítačového systému nebo jeho omezení s cílem zabránit přístupu do systému pojištěného. Za ztrátu z přerušení provozu se považuje snížení čistého zisku, které vzniklo výhradně v důsledku přerušení provozu. Za ztráty z přerušení provozu nelze

považovat: finanční ztráty v důsledku nemožnosti obchodovat, fluktuace hodnoty aktiv, finanční hodnoty na účtech a neschopnost získat úrok.

S kybernetickým útokem mohou vzniknout různé náklady. Podle toho, o jaký druh nákladů se jedná, jsou buď hrazeny z pojištění kybernetických rizik, nebo nejsou hrazeny vůbec. Pojištění Cyber Enterprise Risk Management kryje následující náklady:

- náklady právního zastoupení,
- náklady regulatorního řízení,
- sankce uložené dozorovým orgánem,
- náklady na IT,
- náklady na PR – náprava pověsti pro pojištěné osoby a manažery,
- náklady na obnovu dat – pojištěného a třetích osob.

Pojištění naopak nekryje náklady, které souvisejí s opravou softwarových slabin nebo nedostatků, náklady související se zlepšením počítačového systému, náklady na splnění předpisů na ochranu soukromí nebo daně a pokuty. Každé pojištění má v pojistných podmínkách uvedené výluky, na které se pojištění nevztahuje. V případě pojišťovny Chubb a pojistného produktu Cyber Enterprise Risk Management se jedná o:

- trestné činy společnosti, protiprávní jednání,
- újmy na zdraví nebo věcné škody,
- úmyslné jednání společnosti,
- riziková data neuvedená v dotazníku,
- porušení obchodního tajemství, patentu,
- válka, terorismus.

Pojištění od pojišťovny Chubb se vztahuje na jakékoli nároky a pojistná plnění, která vzniknout kdekoli na světě, s výjimkou Spojených států amerických a Kanady. Ve všeobecných podmínkách jsou definovány limity pojistného plnění a spoluúčast. Pojistné plnění bude poskytnout do maximální výše limitu pojistného plnění dle pojistných podmínek a pojistné smlouvy. Pojistné plnění je poskytováno pouze ve výši, která přesahuje stanovenou spoluúčast. Pojištěný má podle pojistných podmínek oznamovací povinnost. Je povinen pojistiteli oznámit, že vznikla škoda, nárok nebo bylo zahájeno správní řízení. Oznámení musí obsahovat tyto náležitosti:

- popis škody a nákladů a jejich vyčíslení,
- popis protiprávního jednání na něž se pojištění vztahuje,

- identifikaci zúčastněných osob,
- kopie dokumentů, které se týkají správního řízení,
- dokumenty, které si vyžádá pojistitel.

5.2 Colonnade Pojišťovna

Pojišťovna Colonnade nabízí celkem dvě pojištění, která mají souvislost s kybernetickými riziky. Jedná se o pojištění **CYBERPLUS** a pojištění **GDPR**. Pojištění GDPR je více zaměřené na škody a náklady, které se týkají úniku či poškození dat. V rámci toho pojištění je pojištěno následující:

- regulatorní řízení,
- skutečné nebo údajné neoprávněné nakládání s osobními údaji,
- skutečné nebo údajné neoprávněné nakládání s důvěrnými informacemi,
- neoprávněné zpřístupnění osobních dat a informací zaměstnancem společnosti,
- poškození, zničení, odcizení dat ze systému organizace,
- subdodavatelé – jedná se o pochybení subdodavatelské společnosti, která pracuje s osobními či důvěrnými daty.

Díky tomuto pojištění budou pojištěnému uhrazeny náklady na právní ochranu, náklady na regulatorní řízení, náklady na oznámení, náklady na odborné služby nebo sankce a pokuty uložené dozorovým orgánem. Součástí pojištění GDPR jsou také výluky, které jsou uvedené v pojistných podmínkách. Tyto výluky jsou podobné jako u pojištění Cyber Enterprise Risk Management od pojišťovny Chubb. Výluky jsou tyto:

- neoprávněné shromažďování dat,
- jednání proti hospodářské soutěži,
- úmyslné porušení zákona a právních předpisů,
- porušení patentových, licenčních a duševních práv,
- újmy na zdraví a věcné škody
- nároky týkající se cenných papírů,
- riziková data – jedná se o data, která se liší od dat uvedených ve vstupním dotazníku.

Druhým pojistným produktem pojišťovny Colonnade je pojištění CYBERPLUS. Toto pojištění kryje neoprávněné používání osobních a důvěrných dat včetně nákladů na obnovení údajů a IT systémů. Pojištění kybernetických rizik se vztahuje jak na zjevné,

tak i na skryté následky kybernetických rizik. Rozsah pojistného krytí je podobný jako u pojišťovny Chubb. První oblastí, kterou CYBERPLUS pokrývá je **neoprávněné nakládání s údaji**. Pojištění pokrývá náklady a škody, které vznikly důsledkem neoprávněného nakládání s údaji, včetně nákladů na právní zastoupení. V případě, že **subdodavatel**, se kterým má pojištěnec uzavřenou smlouvu o zpracovávání osobních údajů tuto smlouvu poruší, pojistitel hradí vzniklé náklady a škody. Další pojistitelnou oblastí je **zabezpečení sítě**. Pojistitel uhradí škody, které vznikly v důsledku:

- nainstalování nelegálního softwaru, škodlivého kódu nebo viru,
- neoprávněného získání síťového přístupového kódu,
- zničení, pozměnění, vymazání dat ze systému,
- fyzické ztráty IT vybavení společnosti,
- zpřístupnění citlivých dat zaměstnancem společnosti.

Náklady, které jsou vynaložené na odborné služby nebo právní poradenství v oblasti regulatorního řízení jsou hrazeny pouze do výše sublimitu, který je uvedený v konkrétní pojistné smlouvě. Hrazeny jsou i pokuty a sankce, které uložil dozorový orgán, opět pouze do výše sublimitu v pojistné smlouvě. V základní části pojištění CYBERPLUS jsou také zahrnuty **náklady na odborné služby**. Náklady na odborné služby zahrnují: náklady na znalce v oblasti kybernetiky, náklady na nápravu pověsti společnosti, náklady na nápravu dobrého jména jednotlivce, náklady na oznámení a náklady na obnovu elektronických dat.

Pojištění CYBERPLUS se vztahuje i na další pojistitelné oblasti, které již nejsou v základním pojištění, ale lze je připojistit. V pojistných podmínkách společnosti Colonnade jsou označované jako volitelná rozšiřující pojištění. První takovou oblastí je **zveřejnění digitálního obsahu v multimédiích**. Za porušení povinnosti související se zveřejněním digitálního obsahu lze považovat:

- pomluvu, zásah do pověsti právnické nebo fyzické osoby, s tím související citová újma nebo duševní útrapy,
- neúmyslné porušení autorského práva, ochranné známky, loga, sloganu, názvu domény,
- plagiátorství,
- neoprávněné užívání obchodního jména společnosti.

Dle pojistných podmínek se pojištění nevztahuje na ztráty a náklady, které vznikly v důsledku nesprávného ohodnocení zboží nebo výrobku ani na záruky, které se týkají ceny nebo pravosti zboží. Součástí volitelného rozšiřujícího pojištění je také **vydírání prostřednictvím počítačové sítě** a **samotný výpadek sítě**. Za vydírání lze považovat výhružku ohrožením bezpečnosti systému za účelem získání peněžních prostředků. Za ztrátu způsobenou vydíráním lze označit finanční částky, které pojištěný vynaložil na zabránění vydírání či ukončení vydírání. Dále do ztráty spadají náklady na odborné služby, jejichž cílem je vyšetření příčiny vydírání. Součástí pojištění je povinnost důvěrnosti, což znamená, že pojištěný musí zachovávat mlčenlivost o pojištění ztrát způsobených vydíráním. Výpadek sítě lze definovat jako přerušení funkce počítačového systému, které je způsobené selháním zabezpečení. Ztráta způsobená výpadkem sítě znamená snížení čistého zisku a počítá se od uplynutí čekací doby do doby, než se podaří obnovit počítačový systém. Jak je uvedeno v pojistných podmínkách, tato doba může trvat nejdéle 120 dnů od doby, kdy poprvé došlo k výpadku sítě. Za ztráty způsobené výpadkem sítě nelze považovat: ztráty způsobené přerušením externích sítí (elektrické sítě, internet), jakékoli náklady spojené s právním poradenstvím nebo náklady vynaložené na aktualizaci a modernizaci počítačového systému. Pojištěný je povinen do devadesáti dnů od výpadku sítě poskytnout pojistiteli prohlášení, kde jsou uvedené detailní informace týkající se ztrát způsobených výpadkem sítě. Jak již bylo zmíněno u dvou přechozích pojištění, i pojištění CYBERPLUS má v pojistných podmínkách definované výluky. Tyto výluky jsou podobné jako u pojistných produktů Cyber Enterprise Risk Management a pojištění GDPR. Jedná se o:

- jednání proti hospodářské soutěži,
- újmy na zdraví a věcné škody,
- trestné činy a úmyslné jednání,
- smluvní povinnost, smluvní záruky,
- riziková data,
- duševní vlastnictví,
- terorismus, válku,
- neoprávněně shromažďována data.

Oba pojistné produkty od společnosti Colonnade jsou platné po celém světě, nejsou zde žádné výjimky. Sublimity pojistného plnění jsou horní hranicí pojistného plnění pro jednotlivé pojistné události. Tyto sublimity jsou součástí limitu pojistného plnění

a nezvyšují jej. Ztráty a náklady jsou hrazené pouze ve výši, která přesahuje stanovenou spoluúčast. Pojišťovna Colonnade dále poskytuje zachraňovací náklady do výše 25 000 Kč. Colonnade pro své klienty nabízí Cyber Services 24/7. Jedná se o asistenční linku, která je v nepřetržitém provozu a v případě kybernetického incidentu poskytuje okamžitou pomoc od bezpečnostních expertů. Expert klientovi pomůže incident analyzovat a doporučí mu vhodné řešení.

Veškeré ztráty a nároky musí být pojistiteli oznámeny nejpozději poslední den pojistné doby. Oznámení musí obsahovat náležitosti, které se týkají pojistné události. Náležitosti jsou shodné jako u pojišťovny Chubb. Navíc je zde uveden potencionální mediální dopad.

5.3 ČSOB Pojišťovna

Pojištění od pojišťovny ČSOB je upraveno zvláštní a obecnou částí všeobecných pojistných podmínek. První pojistnou oblastí je **skutečné nebo domnělé narušení ochrany dat.** V rámci této oblasti jsou kryty náklady:

- na činnost odborníka, který vyšetřuje kybernetický útok,
- na právní obhajobu,
- na odborníka, který zajišťuje služby PR,
- na zabezpečení služeb na monitorování neoprávněného používání služeb (věrnostní a přístupové karty),
- na práci přesčas, kterou budou vykonávat zaměstnanci centra krizového managementu po dobu 30 dní od pojistné události.

Dále se pojištění vztahuje na **obnovu dat a softwaru po kybernetickém útoku**, na **přerušení nebo omezení provozu**. V tomto případě hradí pojistitel ušlý zisk, stálé náklady a více náklady, které trvají po dobu přerušení nebo omezení provozu. Pojistitel hradí pojištěnému ztráty, které vznikly v důsledku **zaplacení výkupného**, které požadují kybernetičtí útočníci. Toto výkupné je zaplaceno pouze na základě přechozího souhlasu pojistitele. Pojištění dále pokrývá škody, které vznikly přímo v důsledku kybernetického útoku. Dále lze v rámci pojistného produktu od ČSOB pojistit **odpovědnost za újmu vyplývající z porušení ochrany dat** a **odpovědnost za bezpečnost sítí**. Součástí pojištění kybernetických rizik jsou různá výhodná připojištění. Mezi tato připojištění patří:

- **kybernetické vydírání** – v případě, že škody a ztráty způsobené kybernetickým útokem nelze pokrýt z rizika narušení ochrany dat, pojistitel poskytne finanční prostředky na úhradu výkupného a ostatních nákladů.
- **kybernetický zločin** – toto připojištění pokrývá jakékoli finanční prostředky, o které pojištěný přijde v důsledku neoprávněného bankovního převodu.
- **porušení standardů PCI-DSS** – jedná se nedbalost nebo neoprávněný zásah zaměstnance, čímž došlo k selhání zabezpečení sítě.
- **odpovědnost za újmu způsobenou aktivitami v online médiích** – jsou to škody, které vznikly poškozením dobrého jména, pomluvou, porušením obchodních nebo autorských práv.
- **IT asistence i v případě běžné nefunkčnosti IT systémů.**

V pojistných podmínkách pojišťovny ČSOB je uvedeno mnoho výluk a situací, na které se pojištění kybernetických rizik nevztahuje. Tyto výluky jsou charakterem opět velmi podobné jako u výše zmíněných pojistných produktů. Jedná se o:

- majetkové škody a škody na zdraví,
- škody vzniklé úmyslným jednáním pojištěného,
- škody vzniklé v důsledku trestné činnosti,
- terorismus a kybernetický terorismus,
- škody vzniklé v důsledku výpadku infrastruktury dodavatelů (elektrická energie, plyn, internetové služby),
- škodu vzniklá porušením pravidel hospodářské soutěže,
- vynaložené náklady na zlepšení počítačových systémů.

Pojištění kybernetických rizik od ČSOB se vztahuje na veškeré pojistné události, které vznikly kdekoliv po světě. Limity pojistného plnění jsou stanovovány individuálně a jsou uvedeny v pojistné smlouvě. Pojištěný se na pojištění podílí spoluúčastí. V případě že vznikne více pojistných událostí, podílí se pojištěný pouze jednou spoluúčastí, a to tou nejvyšší. Z pojistných podmínek vyplývají nejenom práva, ale také povinnosti pojištěného. Mezi tyto povinnosti patří oznámení pojistné události nejpozději do 15 dnů od doby, kdy škodná událost vznikla. Dále je pojištěný povinen pravidelně zálohovat data (minimálně jednou za týden), mít nainstalovaný software na ochranu před kybernetickými útoky a chránit počítačové systémy. Pojišťovna ČSOB nabízí svým

klientům nepřetržitou pomoc IT odborníků, kteří pomohou v případě kybernetického útoku.

5.4 Kooperativa pojišťovna

Kooperativa je předposlední pojišťovna, která nabízí pojištění kybernetických rizik. Pojištění je upraveno zvláštními a všeobecnými pojistnými podmínkami. První oblast, kterou pojištění pokrývá, je označena jako **škoda na datech** nebo **nefunkčnost počítačového systému**. Jedná se především o poškození, odcizení nebo ztrátu dat z počítačového systému. Pojistitel se zavazuje uhradit náklady na opravu či obnovu dat a dále náklady na uvedení počítačového systému do původního stavu včetně odstranění případného malwaru.

Náklady **regulatorního řízení** se rozumí náklady, které vznikly v důsledku porušení zabezpečení osobních údajů, které byly uložené v systému pojištěného. Porušení zabezpečení bylo vyvoláno kybernetickým útokem. Uhrazeny budou náklady, které byly účelně vynaložené na regulatorní řízení vedené proti pojištěnému. Další pojistitelnou oblastí jsou **vynaložené náklady na PR**. V důsledku kybernetického útoku došlo k oslabení nebo ztrátě důvěryhodnosti. Pojištění následně kryje náklady vynaložené na zveřejnění informací o kybernetickém útoku. V důsledku **přerušení provozu** mohou pojištěnému vzniknout náklady v podobě ušlého zisku a stálých nákladů. Pojištěný je povinen vést evidenci o přerušení provozu, kde bude uvedena příčina a doba trvání přerušení. Poslední pojistnou oblastí je **odpovědnost za újmu**. Finanční újma vznikne neoprávněným zpřístupněním dat z počítačového systému. Poté jsou uhrazeny pojistitelem náklady na řízení před správním orgánem a náklady na obhajobu v trestním řízení. Výluky pojištění kybernetických rizik od pojišťovny Kooperativa jsou následující:

- úmyslné protiprávní jednání,
- újma na zdraví nebo majetku,
- újma způsobená přerušením jakékoli sítě (internetové, elektrické),
- újma v oblasti porušení vlastnických práv a duševního vlastnictví,
- újma za ukončení smluvních vztahů,
- úhrada nákladů za výkupné.

Pojištění pokrývá pojistné události vzniklé v důsledku kybernetického útoku, ke kterému došlo kdekoli na území celého světa. Pojistné plnění je poskytované maximálně do výše

limitu, který je sjednaný v pojistné smlouvě. V případě, že lze následky kybernetického útoku vyřešit různými způsoby, pojistitel poskytne plnění na nejhospodárnější řešení. Pojistné plnění je vypláceno ve výši, která přesahuje sjednanou spoluúčast. V situaci, kdy dojde ke vzniku škody na datech a pojištěný využije služeb IT odborníka určeného pojistitelem, se nepodílí spoluúčastí. U přerušení provozu se sjednává s pojištěným časová spoluúčast. Povinností pojištěného je pojistnou událost telefonicky nahlásit, případně podat písemné oznámení. V případě kybernetického útoku je pojištěný povinen postupovat tak, jak je určené pojistitelem. Tedy využít odsouhlaseného IT technika a zpřístupnit počítačový systém.

5.5 Maxima pojišťovna

Maxima pojišťovna je poslední subjekt, který v České republice poskytuje pojištění kybernetických rizik. Toto pojištění je upraveno zvláštními pojistnými podmínkami. Rozsah pojištění od Maxima pojišťovny lze rozdělit do tří oblastí. První takovou oblastí jsou náklady, které vznikly v souvislosti s **porušením zabezpečení sítě** a **odpovědností za data**. Do těchto nákladů lze zahrnout následující:

- náklady na obnovu dat,
- forenzní náklady,
- výdaje vynaložené na právní zastupování,
- pokuty a náklady v oblasti platebních karet,
- výdaje vynaložené na oznámení a PR,
- náklady spojené s kybernetickým vydíráním.

Druhou oblastí je **ušlý zisk**, který vznikl v důsledku **omezení nebo přerušení provozu**. K omezení nebo přerušení provozu může dojít neoprávněným přístupem, chybou operátora, DDoS útokem nebo zavedením malwaru do IT sítě.

Pojištění se dále vztahuje na **náhradu škod a pokut**, které vznikly v důsledku odpovědnosti za:

- nezabránění DDoS útoku,
- předání malwaru z počítačového systému,
- neoprávněný přístup do počítačového systému,
- ztrátu dat třetí strany nebo neveřejných údajů,
- porušení práva na ochranu osobních údajů a závazku mlčenlivosti.

Pojistitel neposkytne žádné plnění ani úhradu nákladů v následujících případech:

- úhrada škody na zdraví nebo majetku,
- úmyslných trestných činů a podvodných úkonů,
- selhání elektrické, internetové nebo jiné sítě,
- modernizace nebo inovace počítačového systému,
- ztráta nezabezpečených přenosných zařízení,
- zneužití nebo porušení patentu, obchodních práv,
- porušení pravdivého zodpovězení dotazů pojišťovny.

Pojištěný je povinen nahlásit škodnou událost dle postupu, který je uvedený v pojistné smlouvě. Pojištění kybernetických rizik je stejně jako v předchozích případech platné na území celého světa. Limity plnění jsou stanovené v pojistné smlouvě. V případě přerušení provozu je pojistné plnění omezeno dobou ručení. Pojištěný je povinen se na pojištění podílet dohodnout spoluúčastí uvedenou v pojistné smlouvě.

5.6 Srovnání pojištění kybernetických rizik

Tabulka 2 představuje srovnání pojištění kybernetických rizik, které poskytuje výše zmíněných pět pojišťoven. V tabulce jsou uvedeny oblasti, které lze v rámci pojištění krýt a dále je zde uvedeno, zda pojišťovna danou oblast pojišťuje. Z tabulky je patrné, že pojišťovny nabízejí velmi podobné pojistné podmínky, avšak lze nalézt různé odlišnosti v rozsahu pojištění a ve výlukách.

Prvním takovým rozdílem je územní rozsah, na který se pojištění vztahuje. Všechny pojišťovny kromě pojišťovny Chubb nabízejí pojištění kybernetických rizik na území celého světa. Chubb poskytuje krytí na území celého světa s výjimkou Spojených států amerických a Kanady. Všechny pojistné produkty kryjí neoprávněné nakládání s osobními údaji nebo neoprávněné nakládání s důvěrnými korporátními informacemi. Pojišťovna ČSOB tento rozsah pojištění nabízí klientům jako volitelnou možnost. Další rozdíl lze spatřovat v oblastech pojištění dat v papírové podobě, odpovědnosti za subdodavatele a krytí dceřiných společností. Data v papírové podobě nelze pojistit u pojišťovny ČSOB a Kooperativy. Odpovědnost pojištěného za subdodavatele poskytuje Chubb a Colonnade. V případě pojišťovny Chubb se pojištění vztahuje pouze na subdodavatele jako fyzické osoby. U pojišťovny Maxima lze odpovědnost za subdodavatele pojistit na základě individuální dohody. Pojistit dceřiné společnosti nelze

u ČSOB a Kooperativy. V případě ČSOB musí být dceřiné firmy uvedeny explicitně v pojistné smlouvě. Aby bylo možné pojistit dceřinou firmu musí být uvedena v pojistné smlouvě. Tuto podmínku vyžaduje pojišťovna Maxima. Zásadní rozdíl je v krytí sankcí uložených dozorových orgánem. Kromě Kooperativy všechny pojistné produkty tyto sankce pokrývají.

Většina pojistných produktů pokrývá celou řadu nákladů vzniklých v důsledku kybernetického útoku. Jedná se o náklady na IT, náklady na nápravu pověsti, náklady na oznámení a náklady na obnovu dat. Například nápravu pověsti manažerů pokrývají pouze společnosti Chubb a Colonnade. Náklady na obnovu jsou u pojišťovny ČSOB volitelné, podle potřeb klienta. V případě, že byla data smazána důsledkem chybného programu, vzniklé náklady na obnovu dat lze pojistit pouze u pojišťovny Chubb. Náklady na obnovu dat pojištěného vzniklé výpadkem nějaké sítě nelze pojistit ani u jedné pojišťovny.

Oblast kybernetických trestných činů lze pojistit pouze u pojišťovny Chubb a ČSOB. V případě Chubb se jedná o připojištění a u ČSOB lze kybernetické trestné činy pojistit na základě individuálních potřeb klienta. Colonnade a Maxima pojišťovna nabízí připojištění na kybernetické trestné činy. Další významný rozdíl lze nalézt v oblasti pojištění odpovědnosti v souvislosti s médii a vydíráním prostřednictvím počítačové sítě. První i druhou zmíněnou oblast nepojišťuje Colonnade a její produkt pojištění dat a Kooperativa. Poslední pojistitelnou oblastí je přerušení provozu. Tuto oblast pokrývají všechny pojistné produkty kromě pojištění dat od Colonnade. V případě, že přerušení provozu nastane v důsledku přerušení sítě, nelze tento stav pojistit. Pojistná doba krytí v případě přerušení provozu se pohybuje od tří do šesti měsíců.

Tabulka 2: Srovnání rozsahu pojištění

Rozsah pojištění	Chubb	Colonnade Cyberplus	Colonnade GDPR	ČSOB	Kooperativa	Maxima
Neoprávněné nakládání s osobními údaji	ANO	ANO	ANO	ANO	ANO	ANO
Neoprávněné nakládání s důvěrnými korporátními informacemi	ANO	ANO	ANO	ANO	ANO	ANO
Data v papírové podobě	ANO	ANO	ANO	NE	NE	ANO
Odpovědnost za subdodavatele	ANO	ANO	ANO	NE	NE	NE
Zabezpečení sítě	ANO	ANO	ANO	ANO	ANO	ANO
Zpřístupnění dat třetí osob z-cem	ANO	ANO	ANO	ANO	ANO	ANO
Náklady právního zastoupení	ANO	ANO	ANO	ANO	ANO	ANO
Krytí dceřiných firem	ANO	ANO	ANO	NE	NE	ANO
Územní rozsah	Celý svět	Celý svět	Celý svět	Celý svět	Celý svět	Celý svět
Retroaktivita	NE	NE	NE	NE	NE	NE
Náklady regulatorního řízení	ANO	ANO	ANO	ANO	ANO	ANO
Sankce od dozorového orgánu	ANO	ANO	ANO	ANO	NE	ANO
Náklady na IT	ANO	ANO	NE	ANO	ANO	ANO
Náprava pověsti společnosti	ANO	ANO	NE	ANO	ANO	ANO
Náprava pověsti manažerů	ANO	ANO	NE	NE	NE	NE
Náklady na oznámení	ANO	ANO	ANO	ANO	ANO	ANO
Náklady na obnovu dat 3. osoby	ANO	ANO	NE	ANO	ANO	ANO
Náklady na obnovu dat pojištěného	ANO	ANO	NE	ANO	ANO	ANO
Náklady na obnovu dat pojištěného – chyba programu	ANO	NE	NE	NE	NE	NE

Rozsah pojištění	Chubb	Colonnade Cyberplus	Colonnade GDPR	ČSOB	Kooperativa	Maxima
Náklady na obnovu dat pojištěného – výpadek el. energie	NE	NE	NE	NE	NE	NE
Kybernetické trestné činy – odcizení peněz, cenných papírů přes IT systém	ANO připojištění	NE	NE	ANO	NE	NE
Kybernetické trestné činy – social engineering	NE	NE	NE	NE	NE	NE
Neoprávněné užití telekomunikací	ANO připojištění	NE	NE	NE	NE	NE
Odpovědnost v souvislosti s médii	ANO	ANO	NE	ANO	NE	ANO
Vydírání skrz počítačovou síť	ANO	ANO	NE	ANO	NE	ANO
Přerušení provozu	ANO	ANO	NE	ANO	ANO	ANO
Přerušení provozu chybou programu	ANO	ANO	NE	NE	NE	NE
Přerušení provozu výpadkem sítě (energie, internet)	NE	NE	NE	NE	NE	NE
Přerušení provozu – doba krytí	3 měsíce	4 měsíce	NE	90 dnů	Individuálně	180 dnů
Odpovědnost související s přijímáním platebních karet	ANO	NE	NE	NE	NE	ANO

Zdroj: Zpracováno dle interního materiálu společnosti RENOMIA, 2023

Tabulka 3 se zabývá porovnáním výluk u pojištění kybernetických rizik. Výluky blíže specifikují rozsah pojistného krytí. Respektive výluky definují události a podmínky, na které se nevztahuje pojistné plnění. První takovou výlukou, na kterou se pojištění nevztahuje, je jednání proti hospodářské soutěži. Tuto výluky má ve svých pojistných podmínkách uvedený pojistitel Colonnade a ČSOB. Pojištění kybernetických rizik se dále nevztahuje na újmy na zdraví, škody na majetku, smluvní odpovědnost, trestné činy a úmyslná jednání. V případě, že pojištěný neposkytne pojistiteli správné údaje a v dotazníku neuvede riziková data, nemá nárok na pojistné krytí vzniklých škod a ztrát. Rozdíly ve výlukách pojistných produktů lze nalézt například v licenčních poplatcích, nárocích týkajících se cenných papírů, živelných rizik nebo v profesní odpovědnosti. Licenční poplatky nemá ve svých pojistných podmínkách uvedené pojišťovna Kooperativa a Maxima. Živelná rizika jako výluku lze nalézt u ČSOB a Colonnade. Ztrátu nezabezpečených přenosných médií lze pojistit u pojistitelů Chubb, Colonnade a ČSOB. Mezi další výluky patří kryptoměny nebo nároky související s odcizením nebo ztrátou hardwaru.

Z provedené analýzy je patrné, že nabízené pojištění kybernetických rizik od různých pojišťoven si je velmi podobné. Lze konstatovat, že se v základních prvních shoduje. Odlišnosti lze nalézt v některých oblastech pojistného krytí. Například v přerušení provozu nebo v odpovědnosti v souvislosti s médii. Limity pojištění a spoluúčast jsou stanoveny individuálně podle potřeb a požadavků pojištěného. Vše je upraveno v pojistné smlouvě. Výluky pojistného krytí jsou také velmi podobné pro všechny představené pojistné produkty. Individuálně lze sestavit také samotné pojištění kybernetických rizik. Některé pojistitelné oblasti totiž nejsou v základním pojištění. Pojištěný si je tedy může nechat připojistit. Zájemci o pojištění kybernetických rizik mohou buď sami oslovit výše zmíněné pojišťovny, nebo mohou využít služeb zprostředkovatelů pojištění, například společnosti RENOMIA.

Tabulka 3: Porovnání výluk

Výluky	Chubb	Colonnade Cyberplus	Colonnade GDPR	ČSOB	Kooperativa	Maxima
Jednání proti hospodářské soutěži	NE	ANO[1]	ANO	ANO	NE	NE
Újma na zdraví a majetku	ANO	ANO	ANO	ANO	ANO	ANO
Smluvní odpovědnost a záruky	ANO	ANO	ANO	ANO	ANO	ANO
Trestné činy	ANO	ANO	ANO	ANO	ANO	ANO
Riziková data, která nebyla uvedena	ANO	ANO	ANO	ANO	ANO	ANO
Úmyslné jednání	ANO	ANO	ANO	ANO	ANO	ANO
Licenční poplatky	ANO	ANO	ANO	ANO	NE	NE
Předchozí nároky	ANO	ANO	ANO	ANO	ANO	ANO
Nároky týkající se cenných papírů	ANO	ANO	ANO	NE	ANO	NE
Terorismus a válka	ANO	ANO	ANO	ANO	ANO	ANO
Obchodní ztráty na kapitál. trhu	ANO	ANO	ANO	ANO	ANO	NE
Neoprávněně shromážděná data	ANO	ANO	ANO	ANO	ANO	ANO
Výpadek služeb externího dodavatele	ANO	ANO	ANO	ANO	ANO	ANO
Živelná rizika	ANO	NE	NE	NE	ANO	ANO
Porušení obchodního tajemství, patentu	ANO	ANO	ANO	ANO	ANO	ANO
Nárok mezi pojištěnými	ANO	ANO	ANO	ANO	ANO	ANO

[1] ANO – znamená, že daný pojistitel aplikuje dle VPP/ZPP

Výluky	Chubb	Colonnade Cyberplus	Colonnade GDPR	ČSOB	Kooperativa	Maxima
Profesní odpovědnost	NE	NE	NE	ANO	ANO	ANO
Ztráta nezabezpečených přenosných médií	NE	NE	NE	NE	ANO	ANO
Elektronické převody peněz	NE	ANO	ANO	NE	ANO	ANO
Kryptoměny	NE	NE	NE	NE	NE	NE
Nároky v souvislosti přijímání platebních karet	NE	ANO	ANO	NE	ANO	NE
Nároky související s odcizením nebo ztrátou HW	NE	NE	NE	NE	ANO	ANO

Zdroj: Zpracováno dle interního materiálu společnosti RENOMIA, 2023

6 Postup při pojištění kybernetických rizik

Původním záměrem diplomové práce bylo sestavení praktického příkladu. Na tomto příkladu mělo být demonstrováno, zda je pojištění kybernetických rizik výhodné pro společnosti a zda se jim vyplatí tento druh pojištění sjednávat. Cílem bylo uvést dvě situace, první situací mělo být, kolik společnost zaplatí v případě, že se stala obětí kybernetického útoku. V této modelové situaci není sjednáno žádné pojištění kybernetických rizik. Druhá verze měla být obdobná, s tím rozdílem, že napadená společnost by byla pojištěná proti kybernetickým útokům. Tyto dvě situace měly být porovnány a následně měly být vyvozeny závěry. Cílem mělo být zhodnocení výhodnosti pojištění kybernetických rizik pro společnosti. Na doporučení paní ředitelky Ing. Zdeňky Kováříkové společnosti RENOMIA v Plzni bylo od praktického příkladu upuštěno. Bylo zjištěno, že zamýšlený praktický příklad nelze sestavit. Nelze konkrétně stanovit, jak vysoké by společnost platila pojistné. Dále nelze určit, jaké pojistné plnění by bylo v případě kybernetického útoku poskytnuto. Záleží, jakou spoluúčast a pojistné limity by měla společnost sjednané. Dalším významným faktorem je sjednané pojištění kybernetických rizik. Každý pojistný produkt se nepatrně odlišuje a nabízí jiný rozsah krytí. V případě, že nastane kybernetických útok, je pojištěný povinen kontaktovat pojistitele, který má vlastní IT tým na řešení kybernetických incidentů. Tento IT tým rozhoduje o tom, zda se jedná o kybernetický útok, o zaplacení výkupného a dále analyzuje tento útok a pomáhá k minimalizaci následků útoku. Na základě výše zmíněných předpokladů nelze praktický příklad sestavit.

Obsahem této kapitoly bude popis průběhu sjednání pojištění kybernetických rizik včetně charakterizování vstupního dotazníku, bez kterého se nelze pojistit proti kybernetickým rizikům. Následně bude popsáno, jak postupovat v případě, že společnost čelí kybernetickému útoku. Vzor dotazníku bude uveden v přílohách diplomové práce. Tento vzorový dotazník byl poskytnut pro účely diplomové práce od pojišťovací společnosti RENOMIA.

V případě, že se organizace rozhodne pro pojištění kybernetických rizik, prvním krokem je vyplnění vstupního dotazníku, na základě kterého je následně pojištění sjednáno. Dotazník slouží pro shrnutí informací o společnosti a její kybernetické bezpečnosti a poté jako podklad k vypracování návrhu pojištění. Pojištění kybernetických rizik lze sjednat

u výše zmíněných pojišťoven nebo pomocí zprostředkovatelů. Každá pojišťovna má svůj dotazník, mohou se tedy nepatrně lišit.

Dotazník lze rozdělit do několika částí. První část dotazníku se zabývá základními údaji a informacemi o společnosti/pojistníkovi. Vyplňuje se zde název společnosti, sídlo, předmět činnosti, počty klientů a počty zaměstnanců. V případě, že chce pojistník vztahovat pojištění i na dceřiné společnosti, musí uvést jejich názvy, sídla a předměty společnosti. Důležité je také uvést, zda jsou aktiva společnosti nebo její dceřiné společnosti vázané na USA. Třetí a čtvrtá část dotazníku se zabývá finančními údaji a rozsahem pojistné ochrany. Pojistitele zajímá, jaké jsou celkové příjmy organizace. Tyto příjmy jsou rozdělené dle zemí klientů. Tedy na Českou republiku, Evropskou unii, USA/Kanadu a ostatní země. V rozsahu pojistné ochrany se uvádějí výše spoluúčasti a limitů pojistného plnění. Součástí jsou i požadavky na nadstandartní rozsah pojištění.

Následující části dotazníku se již konkrétně zabývají způsobem ochrany dat společnosti, zabezpečením IT sítě a množstvím zpracovávaných dat. V oblasti ochrany osobních údajů se dotazník zaměřuje na to:

- zda společnost podléhá předpisům GDPR,
- zda má vytvořenou vlastní směrnici na ochranu osobních údajů,
- zda jsou osobní data šifrována při ukládání do systémů,
- zda bezpečně nakládá s dokumenty, které obsahují důvěrné informace,
- zda jsou zaměstnanci seznámeni s předpisy o ochraně osobních údajů.

Důležitá informace pro pojistitele je, jaké údaje společnost uchovává a zpracovává a jak tato data chrání. Požaduje uvést po zájemci pojištění také odhadovaný objem zpracovávaných citlivých údajů. V případě, že se chce organizace nechat pojistit v oblasti odpovědnosti v souvislosti s médii, je povinna uvést tyto informace. Jaký druh online činnosti provozuje a zda webové stránky poskytují ochranu soukromí. V oblasti subdodavatelů je důležité uvést, jakou část počítačového systému subdodavatel spravuje. Důležitá je IT bezpečnost. Zde se klade důraz na školení zaměstnanců v oblasti bezpečnosti, na bezpečná hesla a jejich aktualizaci a provádění penetračních testů. Aby mohla být organizace pojištěna, musí mít nainstalované aktuální antivirové programy, používat bezpečností softwary, používat zabezpečená přenosná zařízení a zálohovat data. Poslední část dotazníku se zabývá bezpečnostními incidenty a historií ztrát. Je podstatné

vědět, zda se společnost v minulosti potýkala s narušením bezpečnosti nebo porušením ochrany dat.

Na základě vyplněného dotazníku se pojišťovna rozhodne, zda zájemce pojistí proti kybernetickému riziku. Zájemce o pojištění je povinen dotazník vyplnit pravdivě a o podstatných změnách informovat pojistitele. Dotazník se velmi detailně zabývá IT zabezpečením a analýzou dat, proto je pro společnosti velmi náročné formulář vyplnit.

V případě, že je organizace obětí kybernetického útoku, má povinnost tuto skutečnost nahlásit pojistiteli. Tato povinnost je zakotvena v pojistných podmínkách pojišťoven. Dále existují bezplatné telefonní linky, které poskytují okamžitou pomoc od bezpečnostních expertů. Tato linka funguje na principu nepřetržitého provozu. Jejím cílem je poskytnutí pomoci tak, aby napadená společnost mohla na kybernetický útok zareagovat co nejrychleji a adekvátně. IT odborník podle informací od klienta analyzuje bezpečnostní incident a následně doporučí opatření minimalizující škody. Pojištěné firmy mají možnost si domluvit osobní návštěvu experta přímo v jejich prostorách. Díky zásahu expertů jsou pojistné události řešeny efektivně a pojistné plnění je vypláceno včas. Tito experti rozhodují například o tom, zda má napadená společnost zaplatit výkupné nebo zda byl incident způsoben záměrně.

7 Dotazníkové šetření

Tato kapitola se zabývá výsledky provedeného dotazníkového šetření, které bylo zaměřené na chování obyvatel České republiky v oblasti kybernetických rizik. Cílem dotazníkového šetření bylo zjistit, zda dotazovaní dodržují bezpečnostní zásady a pravidla, díky nimž lze předcházet kybernetickým útokům a zda jsou respondenti pojištění proti kybernetickým rizikům nebo o tom alespoň uvažují.

Dotazník byl rozdělen do dvou sekcí. V první části dotazníku respondenti zodpovídali otázky, které se týkaly identifikačních údajů. Jednalo se o věk a dosažené vzdělání. Druhá část se již zabývala pojištěním kybernetických rizik. Dotazník obsahoval celkem 15 otázek, z nichž převážná většina byla uzavřená a dichotomická. Dále zde byla uvedena jedna otevřená otázka a jedna polootevřená. U otázky číslo 12 bylo možné vybírat více odpovědí.

Dotazník byl spuštěn na dobu dvou měsíců a během této doby ho vyplnilo celkem 341 respondentů. Všechny tyto odpovědi budou dále zpracovávány, žádná odpověď nemusela být vyloučena. Data získaná pomocí dotazníkového šetření lze označit jako data primární. Jedná se o výběrové šetření a data byla získaná jako nahodilý výběr. Cílem bylo získat respondenty ze všech věkových kategorií. Jako metoda pořízení dat bylo zvoleno elektronické dotazování, konkrétně pomocí nástroje Survio. Získaná data byla následně zpracována a vyhodnocena.

Otázka č. 1: Kolik Vám je let?

- Méně než 20 let
- 20–30 let
- 31–40 let
- 41–60 let
- 61 let a více

Respondenti mohli vybírat z celkem pěti kategorií. Cílem bylo získat rovnoměrné zastoupení ze všech věkových skupin. Tento cíl byl naplněn pouze z poloviny. Byli získáni respondenti ve všech věkových kategoriích, avšak zastoupení není rovnoměrně rozdělené. Z celkových 341 respondentů jich je 120 ve věku od 20 do 30 let, což činí 35,2 %. Druhou nejpočetnější skupinou jsou osoby ve věku 31–40 let. Naopak nejméně zastoupenou věkovou kategorií jsou osoby starší 61 let. V tomto věku bylo získáno pouze 7,3 % dotázaných. Data jsou pro přehlednost zobrazena v tabulce níže.

Tabulka 4: Věk respondentů

Věková kategorie	**Odpovědi**	**Relativní podíl**
Méně než 20 let	33	9,7 %
20–30 let	120	35,2 %
31–40 let	92	27 %
41–60 let	71	20,8 %
61 let a více	25	7,3 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 2: Jaké je Vaše nejvyšší dosažené vzdělání?

- Základní
- Středoškolské bez maturity
- Středoškolské s maturitou
- Vyšší odborné
- Vysokoškolské

Nejvíce respondentů, konkrétně 169, uvedlo, že jejich nejvyšší dosažené vzdělání je středoškolské s maturitou. Dalších 84 dotázaných vystudovalo vysokou školu. Naopak nejméně zastoupeným vzděláním je vzdělání základní a vyšší odborné. Základní vzdělání mají tři respondenti z 341 dotázaných. Tito respondenti jsou mladší 20 let nebo ve věkové kategorii 41–60 let. Vyšší odborné vzdělání zvolilo jako odpověď deset osob.

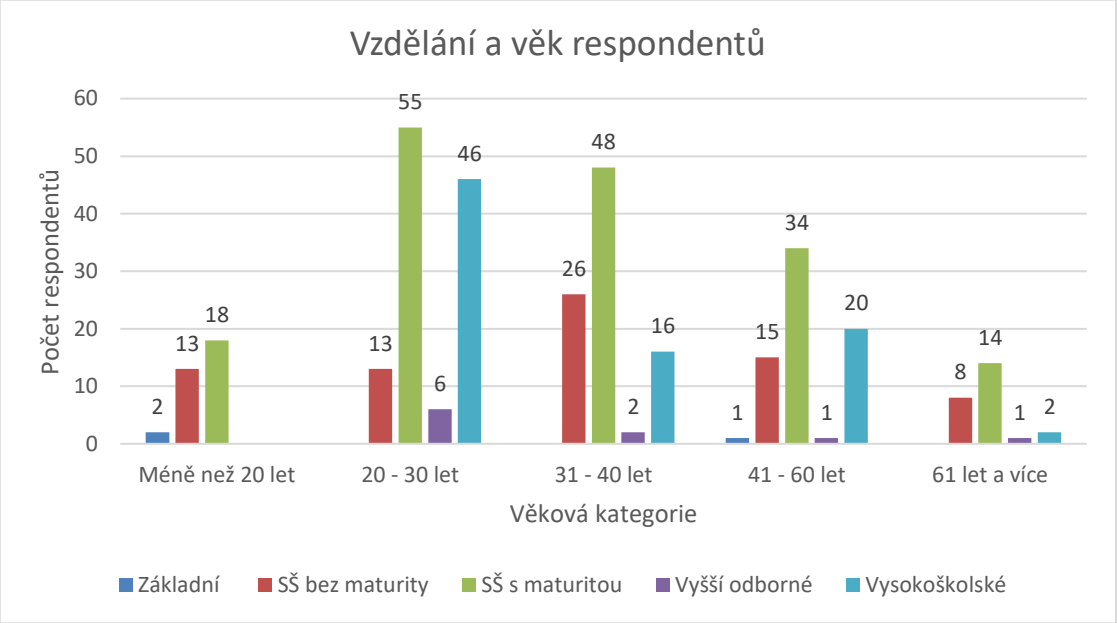
Ze získaných dat lze analyzovat také závislost vzdělání a věku. Dotazovaní, kteří uvedli jako nejvyšší vzdělání středoškolské bez maturity, jsou nejčastěji ve věkové kategorii 31–40 let. Středoškolské vzdělání s maturitou je nejhojněji zastoupené ve věku od 20 do 40 let. Nejvíce vysokoškolsky vzdělaných osob je ve věkové kategorii 20–30 let. Data jsou pro přehlednost zpracována do tabulky a grafu. Na tuto otázku dále navazuje otázka, která se zabývá oborem, ve kterém bylo nejvyšší vzdělání dosaženo.

Tabulka 5: Vzdělání dotazovaných

Druh vzdělání	**Odpovědi**	**Relativní podíl**
Základní	3	0,9 %
Středoškolské bez maturity	75	22 %
Středoškolské s maturitou	169	49,6 %
Vyšší odborné	10	2,9 %
Vysokoškolské	84	24,6 %

Zdroj: Vlastní zpracování, 2023

Obrázek 3: Vzdělání a věk respondentů



Zdroj: Vlastní zpracování, 2023

Otázka č. 3: V jakém oboru je Vaše nejvyšší dosažené vzdělání?

Tato otázka byla otevřená a respondenti měli uvádět, v jakém oboru dosáhli nejvyššího vzdělání. Získaná data bylo třeba rozčlenit do jednotlivých oborů. Někteří respondenti totiž neuváděli obor vzdělání ale přímo konkrétní pracovní pozici. Z dotazníkového šetření vyplývá, že dotazovaní pracují celkem ve 27 různých oborech. Nejvíce zastoupeným oborem je obor ekonomiky. Tuto odpověď zvolilo 41 respondentů, což činí 12,02 %. Druhým nejčastěji zastoupeným oborem je gastronomie, která zahrnuje povolání jako je číšník nebo kuchař. Pod tento obor byly zahrnuty i odpovědi typu hotelnictví a cestovní ruch. Mezi další časté obory patří: obecná příprava (gymnázium), obchod, pedagogika, strojírenství, zdravotnictví a informatika. Někteří respondenti dosáhli svého vzdělání v oborech jako je publicistika, umění nebo chemie. U této otázky bylo shledáno pár nejasností. Šest respondentů uvedlo jako odpověď střední školu a jeden základní školu. Po bližší analýze dat bylo zjištěno, že dva z těchto respondentů jsou mladší 20 let. Tudíž jejich zatím nejvyšší dosažené vzdělání je základní nebo nedokončená střední škola. Zbylí respondenti, kteří zvolili tuto odpověď, jsou ve věkovém rozpětí 20–60 let. Lze předpokládat, že položenou otázku špatně pochopili. Přehled oborů a jejich relativní četnosti jsou uvedeny v tabulce níže.

Tabulka 6: Obory vzdělání

Obor	Odpovědi	Relativní četnost	Obor	Odpovědi	Relativní četnost
Administrativa	7	2,05 %	**Pedagogika**	25	7,33 %
Doprava	8	2,35 %	**Potravinářství**	8	2,35 %
Ekonomika	41	12,02 %	**Právo**	7	2,05 %
Elektrotechnika	8	2,35 %	**Psychologie**	1	0,29 %
Gastronomie	36	10,56 %	**Publicistika**	1	0,29 %
Gymnázium	27	7,92 %	**Stavebnictví**	15	4,40 %
Hutnictví	2	0,59 %	**Strojírenství**	29	8,50 %
Chemie	1	0,29 %	**Textilní výroba a oděvnictví**	1	0,29 %
Informatika	18	5,28 %	**Umění**	6	1,76 %
Jazyky	2	0,59 %	**Veřejnoprávní činnost**	4	1,17 %
Lesnictví	7	2,05 %	**Veterinářství**	1	0,29 %
Marketing	7	2,05 %	**Zdravotnictví**	21	6,16 %
Obchod	23	6,74 %	**Zemědělství**	12	3,52 %
Osobní a provozní služby	16	4,69 %	**Pedagogika**	25	7,33 %
Základní škola	1	0,29 %	**Střední škola**	6	1,76 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 4: Jak podle Vás vypadá dostatečně silné heslo?

- hesloheslo
- 123456789
- 1111111111
- Ko1Le2Di3Pe4Ok5!
- michalnovak

Cílem této otázky bylo zjistit, zda respondenti vědí, jak vypadá bezpečné heslo. Na výběr měli z pěti možností, přičemž čtyři z těchto hesel lze označit jako nebezpečná a nedostatečná. Jak bylo zmíněno v podkapitole Prevence útoků, heslo by mělo být unikátní, silné a neodhadnutelné. Je vhodná kombinace velkých a malých písmen, číslic a speciálních znaků. Jako správnou odpověď měli dotazovaní volit Ko1Le2Di3Pe4Ok5!. Ostatní hesla nejsou vhodná, protože obsahují číselnou posloupnost nebo jméno uživatele.

Z celkových 341 respondentů správně odpovědělo 331, což činí 97,1 %. Lze tedy konstatovat, že drtivá většina dotázaných ví, jak vypadá bezpečné heslo. Čtyři osoby zvolily jako správnou odpověď hesloheslo a dalších šest označilo za bezpečné heslo michalnovak. Respondenti, kteří zvolili tyto odpovědi, jsou ve věkové kategorii od 31 let a více. Vzdělání těchto osob je buď středoškolské bez maturity, nebo středoškolské s maturitou.

Tabulka 7: Bezpečné heslo

Možnost odpovědi	**Odpovědi**	**Relativní podíl**
hesloheslo	4	1,2 %
123456789	0	0 %
1111111111	0	0 %
Ko1Le2Di3Pe4Ok5!	331	97,1 %
michalnovak	6	1,8 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 5: Je tato e-mailová adresa bezpečná a důvěryhodná?

ceskasporitelna@alliance.forspi.com

- Ano
- Ne

Účelem této otázky bylo zjistit, zda jsou respondenti schopni rozpoznat nedůvěryhodnou e-mailovou adresu. Častým útokem totiž bývá zasílání podvodných e-mailů. Cílem těchto útoků je vylákání důvěrných informací od uživatelů, například přihlašovacích údajů do internetového bankovnictví. Tyto e-maily bývají zasílány z podezřelých e-mailových adres. Adresa odesílatele může mít následující podobu: ceskasporitelna@alliance.forspi.com. Je proto klíčové, aby uživatelé kontrolovali, z jaké adresy e-mail přišel. Dále je doporučeno nestahovat z těchto zpráv žádné přílohy ani neotvírat webové odkazy.

97,1 % respondentů výše zmíněnou e-mailovou adresu shledalo jako nebezpečnou a nedůvěryhodnou. Zbylá 3 % dotázaných si myslí, že tato adresa je bezpečná. Tři z těchto respondentů jsou starší 61 let. Senioři bývají na internetu méně obezřetní, a proto se stávají snadným terčem kybernetických útoků. Na tuto otázku navazuje otázka číslo 6, která se respondentů ptá, zda by zadali přihlašovací údaje k bankovnictví do odkazu, který by přišel z výše uvedené adresy.

Tabulka 8: Je e-mailová adresa bezpečná a důvěryhodná

Možnost odpovědi	**Odpovědi**	**Relativní podíl**
Ano	331	97,1 %
Ne	10	2,9 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 6: Zadali byste přihlašovací údaje k internetovému bankovnictví do odkazu, který by přišel z výše uvedené e-mailové adresy?

- Ano
- Ne

339 respondentů uvedlo, že by do odkazu své přihlašovací údaje nezadali. Zbylé dvě osoby by zřejmě čelily kybernetickému útoku, protože by přihlašovací údaje do odkazu zadaly. Tito dva dotázaní jsou ve věkové kategorii 20–30 let a 61 let a více. Zajímavým zjištěním je fakt, že osoby, které v předchozí otázce označily e-mailovou adresu za důvěryhodnou, by do odkazu i přesto nezadaly přihlašovací údaje k internetovému bankovnictví. Pouze jediný respondent označil e-mailovou adresu za bezpečnou a zároveň by do odkazu zadal přihlašovací údaje.

Tabulka 9: Přihlašovací údaje

Možnost odpovědi	**Odpovědi**	**Relativní podíl**
Ano	339	99,4 %
Ne	2	0,6 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 7: Máte ve všech Vašich zařízeních (mobilní telefon, tablet, počítač) nainstalované aktuální antivirové programy?

- Ano, ve všech
- Ne, nemám
- Pouze v některých

Důležitým bezpečnostním opatřením je mít aktualizované antivirové programy ve všech používaných elektronických zařízeních. Díky tomu lze předcházet kybernetickým útokům a vyhnout se tak odcizení dat. Více jak polovina dotázaných aktualizuje antivirové programy ve svých zařízeních pravidelně. Dalších 96 respondentů aktualizuje ochranné programy pouze v některých elektronických zařízeních. 66 osob se aktualizací vůbec nezabývá, čímž se vystavuje kybernetickému riziku.

Tabulka 10: Aktualizace antivirových programů

Možnost odpovědi	**Odpovědi**	**Relativní podíl**
Ano, ve všech	179	52,5 %
Ne, nemám	66	19,4 %
Pouze v některých	96	28,2 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 8: Zálohujete pravidelně svá data?

- Ano, pravidelně
- Ne, nezálohuji
- Ano, nepravidelně

Zálohování dat je velmi důležitá činnost, protože díky záloze nemusí uživatelé nebo podniky přijít o data v důsledku kybernetického útoku. Je důležité data správně zálohovat a spravovat. Data lze zálohovat na externí zařízení nebo na cloudové servery.

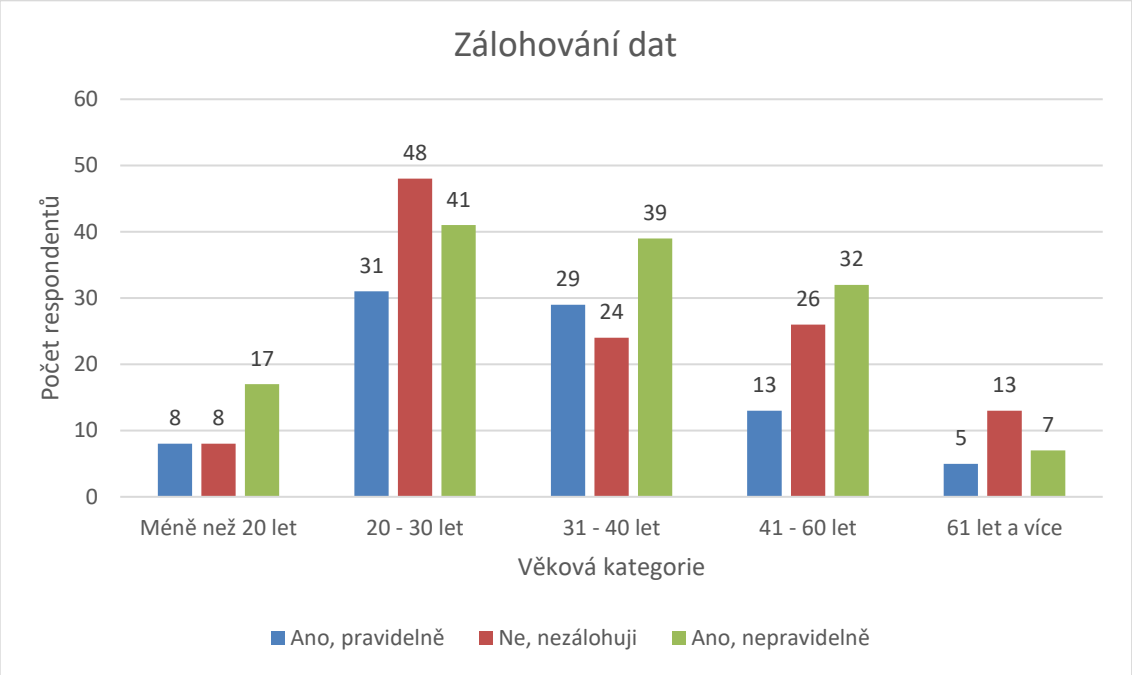
Podle dotazníkové šetření svá data pravidelně zálohuje pouze 25,2 % respondentů. Téměř jedna třetina osob (34,9 %) uvedla, že nezálohuje data vůbec. Tím se vystavují riziku ztráty důležitých údajů. Zbylých 39,9 %, což je 136 osob, zálohuje data alespoň nepravidelně. Bližší analýza ukázala, že nejméně zálohují osoby ve věku 20–30 let. 48 respondentů z této věkové kategorie nezálohuje data vůbec a 41 uvedlo, že zálohují data nepravidelně.

Tabulka 11: Zálohování dat

Možnost odpovědi	Odpovědi	Relativní podíl
Ano, pravidelně	86	25,2 %
Ne, nezálohuji	119	34,9 %
Ano, nepravidelně	136	39,9 %

Zdroj: Vlastní zpracování, 2023

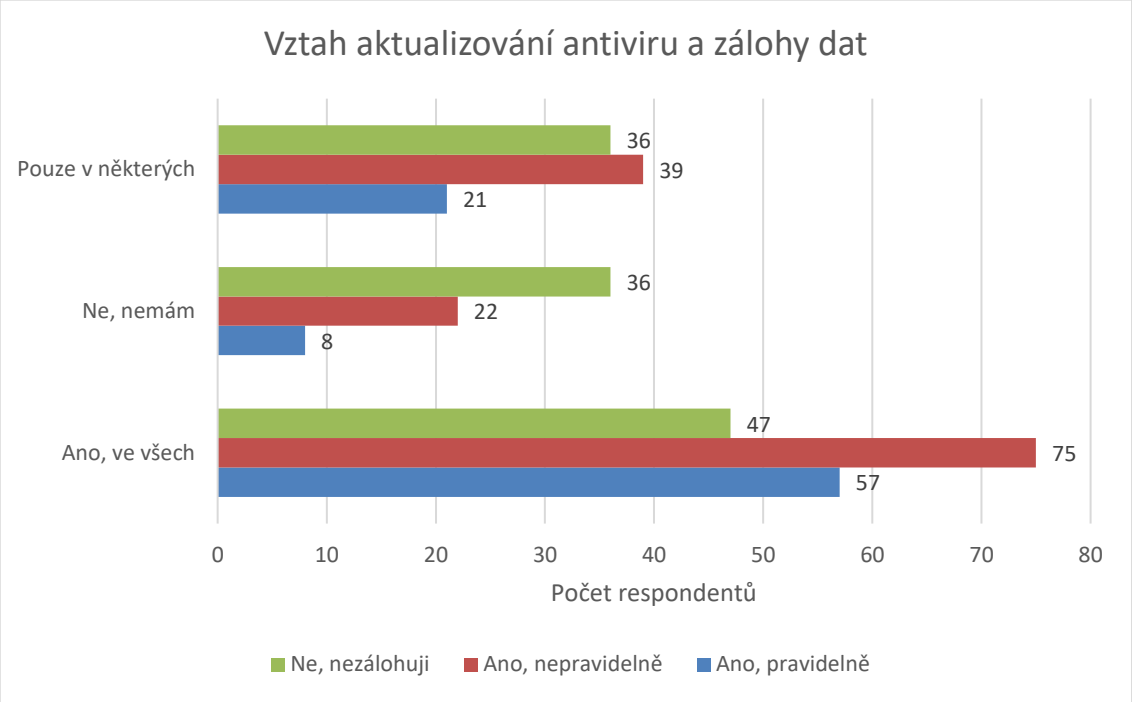
Obrázek 4: Zálohování dat podle věku



Zdroj: Vlastní zpracování, 2023

Pomocí kontingenční tabulky byl vyhodnocen vztah mezi pravidelným aktualizováním antivirových programů a zálohováním dat. Z Obrázku 3 je patrné, že osoby, které pravidelně antivir aktualizují, svá data zálohují buď to pravidelně, nebo nepravidelně. Opak lze spatřit v případě, kdy respondenti nezálohují svá data, tak nemají ani aktuální ochranné programy. Pokud dotazování mají aktuální ochranný systém nainstalovaný pouze v některých zařízeních, tak zpravidla svá data zálohují na nepravidelné bázi nebo vůbec nezálohují.

Obrázek 5: Vztah aktualizace antiviru a zálohování dat



Zdroj: Vlastní zpracování, 2023

Otázka č. 9: Sdělil/a jste někomu přihlašovací údaje k internetovému bankovnictví nebo PIN karty?

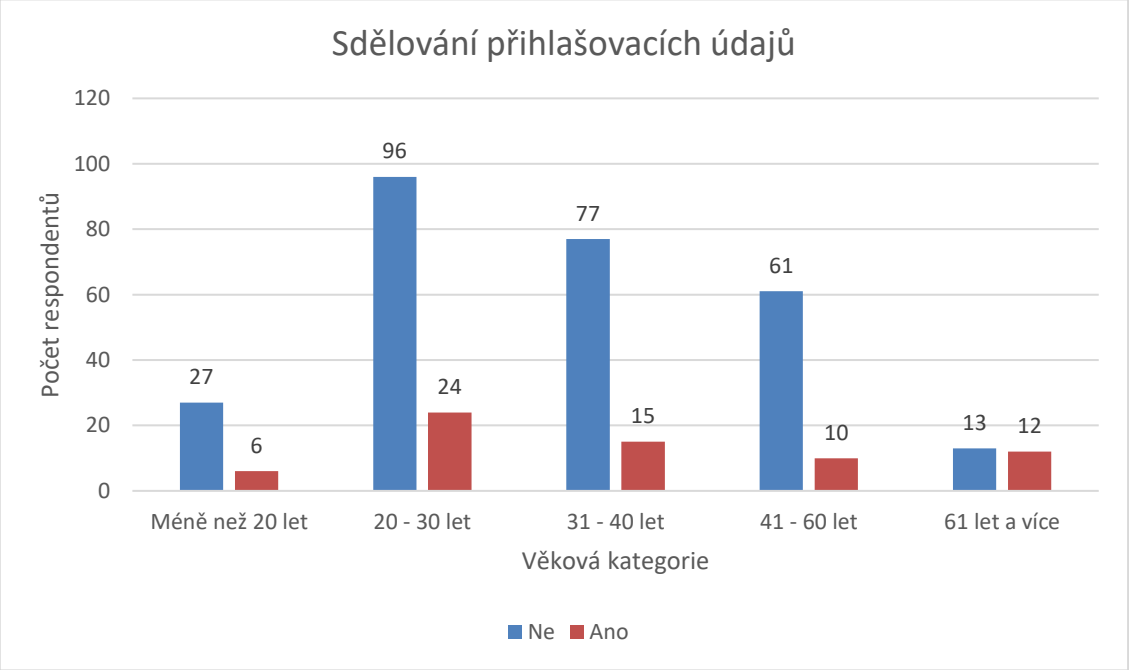
- Ano
- Ne

Otázka č. 10: Ukládáte si přihlašovací údaje do internetových prohlížečů?

- Ano
- Ne

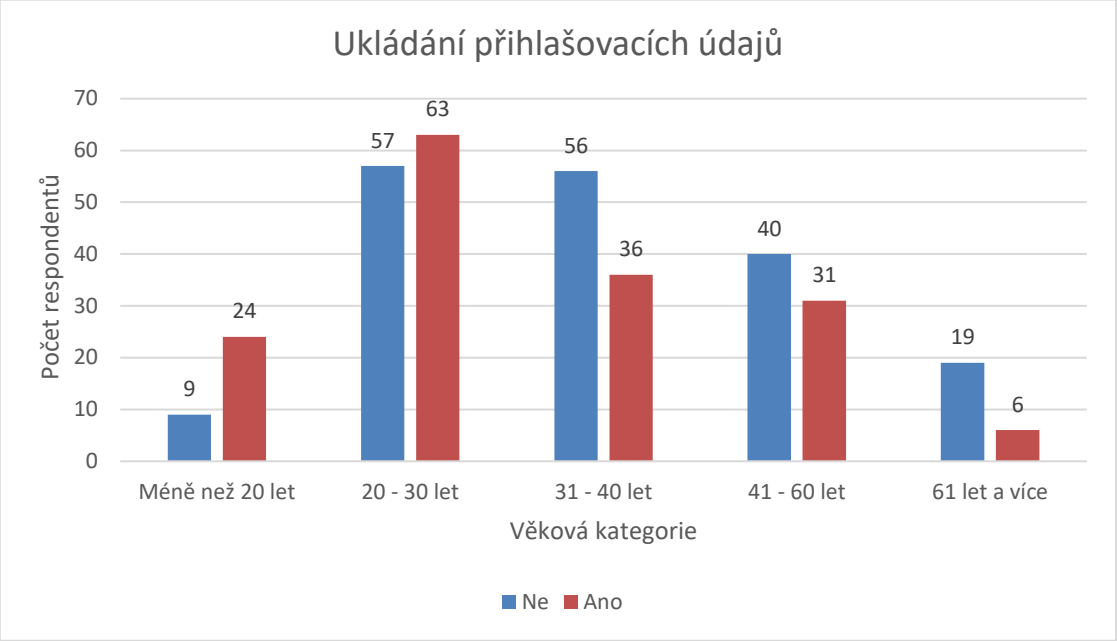
Sdělování přihlašovacích údajů k bankovnictví nebo PINu cizím osobám je velmi rizikové. Tyto osoby mohou údaje snadno zneužít a odcizit například finanční prostředky z účtu. Přes 80 % dotázaných, konkrétně 274 osob uvedlo, že přihlašovací údaje nikomu nesdělily. 67 respondentů poskytlo citlivé údaje další osobě. Nejvíce dotázaných, kteří sdělují přihlašovací údaje nebo PIN, je ve věku od 20 do 30 let. S bezpečností na internetu dále souvisí ukládání přihlašovacích údajů do internetových prohlížečů. Z 341 dotázaných ukládá údaje do prohlížečů 160 osob. Tyto osoby jsou nejčastěji ve věku od 20 do 30 let a 31–40 let.

Obrázek 6: Sdělování přihlašovacích údajů podle věku



Zdroj: Vlastní zpracování, 2023

Obrázek 7: Ukládání přihlašovacích údajů podle věku



Zdroj: Vlastní zpracování, 2023

Otázka č. 11: Používáte k placení mobilní telefon?

- Ano
- Ne

Otázka č. 12: Jaké ověření používáte při placení mobilním telefonem?

- Otisk prstu
- PIN kód
- Scan obličeje
- Znak
- Heslo
- Žádné
- Jiné

Otázka č. 11 byla filtrační a v případě, že na ní respondent odpověděl ne, byl automaticky přesměrován na otázku č. 13. Přesně 200 dotazovaných tedy 58,7 % odpovědělo, že k placení využívá mobilní telefon. Zbylých 141 respondentů telefon k placení nepoužívá. Telefon upřednostňují k placení především osoby ve věku od 20 do 30 let. Naopak nejméně využívaný je u osob mladších 20 let nebo starších 61 let.

Při používání mobilního telefonu je důležité používat správné zabezpečení. Za nejbezpečnější způsob lze považovat dvojité ověření. Celkem 93 respondentů využívá na svých mobilních zařízeních dvojité zabezpečení. Většina těchto dotázaných používá k ověření plateb biometrické údaje, tedy otisk prstu nebo scan obličeje a dále PIN kód.

Z dotazníkové šetření vyplývá, že respondenti k ověření nejčastěji používají otisk prstu (85), PIN kód (78) a scan obličeje (71). Mezi méně časté patří znak a heslo. Čtyři dotazovaní dokonce uvedli, že k ověření plateb při placení mobilním telefonem nepoužívají žádnou z výše zmíněných možností. Tyto osoby jsou ve věku od 20 do 40 let a mají středoškolské nebo vysokoškolské vzdělání.

Tabulka 12: Ověření při platbě telefonem

Možnost odpovědi	Odpovědi	Relativní podíl
Otisk prstu	85	42,5 %
PIN kód	78	39 %
Scan obličeje	71	35,5 %
Znak	34	17 %
Heslo	34	17 %
Žádné	4	2 %
Jiné	0	0 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 13: Byl/a jste někdy terčem kybernetického útoku?

- Ano
- Ne

Poslední část dotazníkového šetření se zabývala tím, zda jsou respondenti pojištění proti kybernetickému riziku nebo o tom alespoň uvažují. Celkem 42 dotazovaných uvedlo, že někdy čelili kybernetickému útoku. Pouze šest z těchto 42 je pojištěných proti kybernetickému riziku. Dalších devět uvedlo, že uvažují o pojištění kybernetických rizik. Většina osob, které čelily kybernetickému útoku je ve věku 20 – 30 let a 41 – 60 let. Zbylých 299 dotázaných nikdy nebylo obětí kybernetického útoku.

Tabulka 13: Oběti kybernetického útoku

Možnost odpovědi	Odpovědi	Relativní podíl
Ano	42	12,3 %
Ne	299	87,7 %

Zdroj: Vlastní zpracování, 2023

Otázka č. 14: Jste pojištěný/á proti kybernetickému riziku?

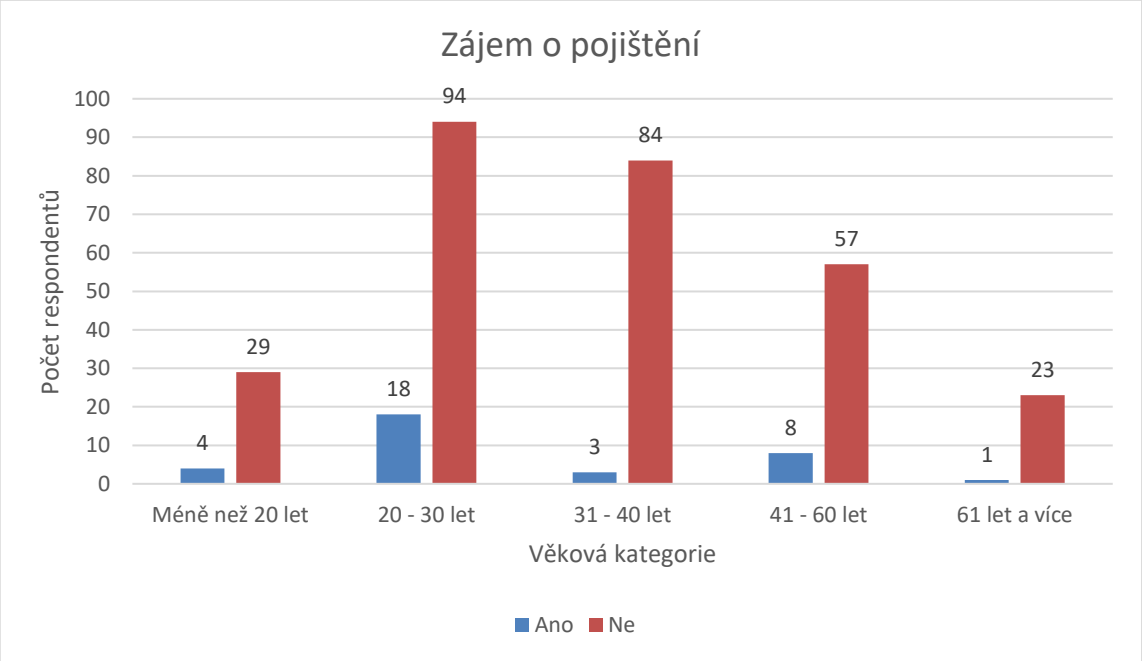
- Ano
- Ne

Otázka č. 15: Uvažujete o tom, že se necháte proti kybernetickému riziku pojistit?

- Ano
- Ne

Proti kybernetickému riziku je ze všech dotázaných pojištěno pouze 20 osob. Lze se domnívat, že tyto osoby mají pojištění kybernetických rizik sjednané v rámci pojištění domácnosti. Protože pojištění kybernetických rizik pro jednotlivce je nabízeno pouze v rámci pojištění domácnosti, nejedná se tedy o samostatný pojistný produkt. Tyto osoby spadají převážně do věkové kategorie od 20 do 30 let. Otázka 14 byla filtrační. Pokud respondent uvedl, že je pojištěný proti kybernetickému riziku, již nebylo dotazován, zda o pojištění uvažuje. 10,6 % respondentů, tedy 34 osob, uvedlo, že alespoň uvažují o pojištění kybernetických rizik. Více jak polovina těchto osob je opět ve věku od 20 do 30 let.

Obrázek 8: Zájem o pojištění



Zdroj: Vlastní zpracování, 2023

7.1 Zhodnocení dotazníkového šetření

Provedeného dotazníkového šetření se zúčastnilo celkem 341 respondentů. Tyto zúčastněné osoby zastupují všechny věkové kategorie. Nejvíce dotázaných bylo ve věkové kategorie 20–30 let. Naopak osoby starší 61 let odpovídaly v dotazníkovém šetření nejméně. Nejrozšířenějším vzděláním mezi respondenty je středoškolské s maturitou, které je následované vysokoškolským a středoškolským bez maturity. Obory nejvyššího dosaženého vzdělání byly velmi rozmanité. Bylo uvedeno celkem 27 různých oborů. Nejčastěji zastoupeným oborem byla ekonomika, gastronomie a obecná příprava, tedy gymnázium. Lze nalézt i netypické obory jako je hutnictví nebo chemie.

Další otázky uvedené v dotazníku se již zabývaly chováním obyvatel České republiky v oblasti kybernetických rizik. Otázky byly zaměřené na znalost respondentů v oblasti bezpečnosti na internetu. Drtivá většina dotázaných osob dokázala z pěti nabízených hesel označit to správné, které je bezpečné a neprolomitelné. V následující otázce se respondenti měli rozhodnout, zda je e-mailová adresa důvěrná či nikoli. To se podařilo 331 osobám z 341 dotázaných. Žádný z respondentů by do odkazu, který by přišel z této e-mailové adresy nezadal přihlašovací údaje k internetovému bankovnictví. Více jak polovina dotázaných pravidelně aktualizuje antivirovou ochranu ve všech elektronických zařízeních. V oblasti zálohování dat jsou výsledky šetření poněkud horší. Pouze 86 osob z 341 pravidelně zálohuje svá data, tedy alespoň jednou za měsíc. Na otázku, zda sdělují přihlašovací údaje nebo PIN cizím osobám odpovědělo 274 respondentů, že nikoli. Téměř polovina respondentů ukládá přihlašovací údaje do webových prohlížečů. Mobilní telefon používá k placení 200 osob. K ověření plateb mobilním telefonem nejčastěji dotazovaní využívají biometrické údaje a PIN kód. 12,3 % respondentů ve svém životě čelilo kybernetickému útoku. Proti kybernetickému útoku je pojištěno pouhých 20 osob a dalších 34 osob o pojištění alespoň uvažuje.

Bylo zjištěno, že dotazovaní mají přehled, jak vypadá bezpečné heslo, nezadávají citlivé informace do podezřelých odkazů. Avšak v oblasti aktualizování ochranných programů a zálohy dat by měli být dotazovaní pečlivější a obezřetnější. Také by neměli ukládat přihlašovací údaje do internetových prohlížečů. Při placení telefonem využívají ve většině případů biometrické údaje, což je nejbezpečnější způsob ochrany. V oblasti pojištění proti kybernetickým rizikům mají respondenti spíše negativní postoj. Tento

negativní postoj může být způsoben nevědomostí a neznalostí pojistného produktu pojištění kybernetických rizik.

8 Budoucí vývoj

Ve světě je denně provedeno 35 – 50 milionů hackerských útoků. Kybernetickým útokům čelí nejčastěji tato odvětví: průmysl, služby, finanční instituce, věda a vzdělání, vládní instituce, zdravotnictví. Zdravotnická zařízení si nemohou dovolit výpadek služeb nebo ztrátu citlivých údajů pacientů. Posledním takovým případem v České republice je nemocnice v Benešově. Ta byla napadena ransomware a více než měsíc trvalo obnovení IT systémů. Škoda byla vyčíslena na 40 milionů Kč. Útoku dále čelila například společnost OKD, Správa Pražského hradu a v nedávné době také společnost ČSOB.

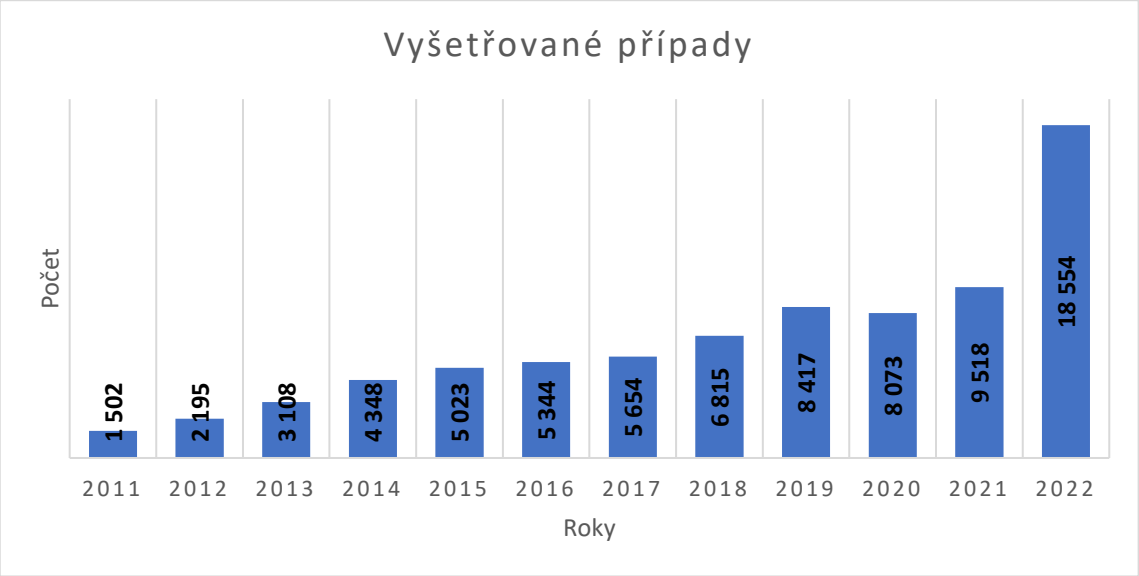
Až 58 % kybernetických útoků je prováděno hackerskými skupinami z Ruska. Mezi země, které nejčastěji čelí útokům patří USA, Ukrajina, Belgie nebo Spojené království. Stále častější jsou útoky, které jsou zaměřené na získání citlivých údajů. Díky těmto údajům mohou mít země například lepší pozici v informační válce. Celosvětově činil meziroční nárůst kybernetických útoků 31 %.

V České republice byl meziroční nárůst kybernetických útoků 20 %. Říjen roku 2022 se stal měsícem s největším počtem útoků. Národní úřad pro kybernetickou bezpečnost zaznamenal za tento měsíc celkem 20 incidentů. Ze zprávy NÚKIB za rok 2020 vyplývá, že bylo nahlášeno celkem 468 incidentů, 99 z nich řešil NÚKIB. Národní bezpečnostní tým České republiky CSIRT řešil v roce 2020 1267 bezpečnostních incidentů. V roce 2021 bylo nahlášeno 476 incidentů. 157 jich muselo být řešeno Národním úřadem pro kybernetickou a informační bezpečnost. CSIRT se v roce 2021 zabýval celkem 1726 bezpečnostními incidenty. Z výše uvedeného vyplývá, že kybernetické útoky a incidenty meziročně vzrůstají. Z obrázku 9 je patrné, že Policie ČR každým rokem řeší čím dál více kyberkriminálních případů. V roce 2022 bylo zaznamenáno 18 554 případů, což je oproti přechozímu roku dvojnásobek.

Na růstu kybernetických útoků se podílí řada faktorů. Jedná se především o snadnější dostupnost a automatizaci nástrojů, které útočníci využívají. Mezi další faktory patří rozvoj moderních technologií a IT systémů, vyšší výpočetní výkon systémů a také to, že aktiva v kyberprostoru jsou stále cennější. Kvůli těmto okolnostem bude přibývat kybernetických útoků a bude se zvyšovat jejich sofistikovanost. Na tento vývoj kybernetických útoků reagují firmy a investují do zabezpečení systémů a kyberochrany. To bohužel neplatí pro ČR, kde manažeři firem kybernetickým útokům nevěnují dostatečnou pozornost. Změnu v kybernetické bezpečnosti přinese nová směrnice

Evropské unie NIS 2. Díky této směrnici budou muset firmy zvýšit úroveň kybernetické bezpečnosti. Dalším opatřením Evropské unie je nařízení DORA. Toto nařízení se bude týkat především finančního sektoru. Tyto subjekty budou muset dokázat, že jsou schopné čelit kybernetickému útoku a následně hrozbu vyřešit. Je zřejmé, že kybernetických útoků a incidentů bude přibývat, proto je nezbytné se umět před těmito hrozbami chránit.

Obrázek 9:Vyšetřované kyberkriminální případy



Zdroj: Zpráva o stavu kybernetické bezpečnosti, 2021

Závěr

V předložené diplomové práci byl podán přehled o kybernetických rizicích a kybernetických útocích. Následně byla zmapována stručná historie pojištění kybernetických rizik a legislativa upravující toto pojištění. Praktická část se zabývala porovnáním a následným zhodnocením produktové nabídky vybraných komerčních pojišťoven. Dále bylo zmapováno chování obyvatel České republiky v oblasti kybernetických rizik pomocí dotazníkového šetření.

Dle barometru rizik se kybernetické riziko v posledních dvou letech umisťuje na předních příčkách mezi všemi ostatními riziky. Každým rokem přibývá kybernetických útoků, které bývají sofistikovanější a hůře odhalitelné. Mezi nejčastější útoky patří phishinig, malware a DDoS útok. Je zapotřebí se proti hackerským útokům bránit dodržováním bezpečnostních zásad a dále pomocí pojištění kybernetických rizik. V současné době manažeři společností nepřikládají kybernetickému riziku velkou pozornost a jejich firmy tak nejsou dostatečně zabezpečeny.

Z rozboru pojistných produktů vybraných pojišťoven vyplývá, že jsou tyto produkty velmi podobné a lze u nich nalézt pouze nepatrné odlišnosti. Liší se například v územním rozsahu krytí, v pojištění dceřiných společností nebo odpovědnosti za subdodavatele. Rozdíly lze spatřit i ve výlukách, kde například jednání proti hospodářské soutěži mají v pojistných podmínkách uvedeny pouze dvě pojišťovny. Pojištění kybernetických rizik lze sestavit individuálně podle potřeb klienta.

Z dotazníkového šetření vyplývá, že respondenti jsou seznámeni s bezpečnostními zásadami, díky kterým se chrání proti kybernetickým útokům. Většina dotázaných byla schopná označit silné heslo a dále rozpoznali podezřelou e-mailovou adresu. V oblasti aktualizace antivirových programů a zálohy dat lze spatřit bezpečnostní riziko. Respondenti často nepoužívají aktuální antiviry a svá data zálohují nepravidelně nebo vůbec. Při placení telefonem jsou dotázání obezřetní a používají správné zabezpečení. Jen několik respondentů se stalo obětí kybernetického útoku. Většina těchto osob se ani po zkušenosti s kybernetickým útokem nenechala proti kybernetickým rizikům pojistit. Některé dotázané osoby o pojištění alespoň uvažují. A pouze 20 respondentů je pojištěno.

Lze očekávat, že kybernetické útoky budou každým rokem narůstat. Proto je důležité, aby společnosti i jedinci věděli, jak se proti těmto hrozbám chránit.

Seznam použité literatury

Monografie

Arnold, R. (2017). *Cybersecurity: A Business Solution*. Threat Sketch.

Cipra, T. (2015). *Riziko ve financích a pojišťovnictví: Basel III a Solvency II*. Ekopress.

Doucek, P., Konečný, M., & Novák, L. (2019). *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Professional Publishing.

Ducháčková, E. (2015). *Pojištění a pojišťovnictví.* Ekopress.

Ducháčková, E. (2009). *Principy pojištění a pojišťovnictví*. (3. vyd.). Ekopress.

Ducháčková, E., & Daňhel, J. (2012). *Pojistné trhy*. Professional Publishing.

Ducháčková, E., & Daňhel, J. (2010). *Teorie pojistných trhů*. Professional Publishing.

Jirásek, P., Novák, L. & Požár. (2013). *Výkladový slovník kybernetické bezpečnosti*. Policejní Akademie.

Jirovský, V. (2007). *Kybernetická kriminalita.* Grada.

Hromada, M., Hrůza, P., Kaderka, J., Luňáček, O., Nečas, M., Ptáček, B., Skoruša, L., & Složil, R. (2015). *Kybernetická bezpečnost: teorie a praxe*. Powerprint.

Řezáč, F. (2011). *Řízení rizik v pojišťovnictví*. Munipress.

Časopisy

Duračinská, Z. (2016). Co přináší nová směrnice EU o síťové a informační bezpečnosti. *IT Systems 2016* (10), 2-3.

Plecháček, P. & Dudková, R., K. (2022). DORA anebo jednotná pravidla a stabilita pro IT ve finančním sektoru. *Bankovnictví 29* (9), 20-21.

Dobiáš, P. (2018). Pojištění kybernetických rizik. *Pojistný obzor 2018* (2), 18-20.

Zákony a vyhlášky

Zákon č. 181/2014 Sb.

Zákon č. 277/2009 Sb.

Vyhláška č. 82/2018 Sb.

Zákon č. 89/2012 Sb.

Elektronické zdroje

AEC (2023). *Služby informační bezpečnosti*. Dostupné 10. 1. 2023 z https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjA5_vd0cn9AhUgVvEDHWPTCKQQFnoECAsQAQ&url=https%3A%2F%2Fwww.aec.cz%2Fcz%2FDocuments%2FFiles%2FAEC-Advanced-Persistent-Thread.pdf&usg=AOvVaw3evQZ0bkBKH4pYXJs16f-d

Allianz (2022). *Allianz Risk Barometer 2022*. Dostupné 15. 11. 2022 z https://www.allianz.cz/cs_CZ/pojisteni/vse-o-allianz/centrum-clanku/allianz-risk-barometer-2022.html

Allianz (2023). *Making noise about "silent" cyber*. Dostupné 7. 3. 2022 z https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/silent-cyber.html

Avast (2022). *Ochrana před hrozbami na Internetu*. Dostupné 29. 11. 2022 z https://www.avast.com/cs-cz/c-online-threats

Axians (2022). *Jak probíhá kybernetický útok? Kybernetická bezpečnost*. Dostupné 28. 11. 2022 z https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/

Bezpečnost práce (2022). *Kybernetická bezpečnost ve firmách. Tři pilíře pro ochranu před kyberútoky.* Dostupné 1. 3. 2022 z https://www.bozp.cz/aktuality/kyberneticka-bezpecnost-ve-firmach/

ColonyWest (2023). *A History of Cyber Liability Insurance*. Dostupné 4. 3. 2023 z https://colony-west.com/a-history-of-cyber-liability-insurance/

Čermák, M. (2015). *APT: Jak probíhá cílený útok.* CleverAndSmart. Dostupné 21. 2. 2023 z https://www.cleverandsmart.cz/apt-jak-probiha-cileny-utok/

Česká asociace pojišťoven (2022). *Slovnikenc*. https://www.cap.cz/slovnikenc

Česká bankovní asociace (2021). *Pojistná smlouva - Finanční vzdělávání*. Dostupné 20. 11. 2022 z https://www.financnivzdelavani.cz/svet-financi/pojistovnictvi/pojistna-smlouva

Česká bankovní asociace (2023). *Desatero bezpečnosti na internetu*. Kybertest.cz. Dostupné 28. 2. 2023 z https://www.kybertest.cz/desatero-bezpecnosti-na-internetu

Česká spořitelna (2023). *Jak si zvolím bezpečný PIN pro aplikaci George klíč?* Dostupné 28. 2. 2023 z https://www.csas.cz/cs/caste-dotazy/jak-si-zvolim-bezpecny-pin-pro-aplikaci-george-klic

ČSOB Pojišťovna (2022a). *Pojistník - ČSOB Pojišťovna*. https://www.csobpoj.cz/slovnik-pojmu/pojistnik

ČSOB Pojišťovna (2022b). *Obmyšlený – ČSOB.* Pojišťovna. https://www.csobpoj.cz/slovnik-pojmu/obmysleny

ČSOB Pojišťovna (2022c). *Poškozený - ČSOB Pojišťovna*. https://www.csobpoj.cz/slovnik-pojmu/poskozeny

Deloitte (2021). *Global risk management survey, 12th edition*. Dostupné 15. 11. 2022 z https://www2.deloitte.com/us/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html

Deloitte (2023). *Global future of Cyber Survey 2023*. Dostupné 7. 3. 2023 z https://www2.deloitte.com/cz/cs/pages/risk/articles/global-future-of-cyber-survey.html

Digitální pevnost (2023). *DDoS – frontální útok na váš web nebo e-mail*. Dostupné 21. 2. 2023 z https://www.digitalnipevnost.cz/viki/ddos-distributed-denial-service

Digitální pevnost (2019). *Smartphone je snadným terčem útoku: čím a jak ho chránit?* Dostupné 28. 2. 2023 z https://www.digitalnipevnost.cz/zpravodaj/detail/jak-ochranit-smartphone

EIOPA (2019). *Cyber risk forinsurers–challenges and opportunities*. Publications Office of the European Union.

ESET (2022). *Co je počítačový virus + Druhy virů*. Dostupné 30. 11. 2022 z https://www.eset.com/cz/virus/

ESET (2023a). *Co je DDoS útok a jaká je ochrana?* Dostupné 21. 2. 2023 z https://www.eset.com/cz/ddos-utok/

ESET (2023b). *Co je to antivirus a antivirový program*? Dostupné 28. 2. 2023 z https://www.eset.com/cz/antivirus-software/

ESET (2023c). *Zhodnocení stavu bezpečnosti*. Dostupné 1. 3. 2023 z https://www.eset.com/cz/firmy/eset-services/bezpecnostni-audit/zhodnoceni-stavu-bezpecnosti

Evropská rada (2022a). *Kybernetická bezpečnost: jak EU řeší kybernetické hrozby – Consilium*. Dostupné 5. 11. 2022 z https://www.consilium.europa.eu/cs/policies/cybersecurity/

Evropská rada (2022b). *EU se rozhodla posílit kybernetickou bezpečnost a odolnost v celé Unii*. Dostupné 5. 3. 2023 z https://www.consilium.europa.eu/cs/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Evropská rada (2023). *Obecné nařízení o ochraně údajů*. Dostupné 1. 3. 2023 z https://www.consilium.europa.eu/cs/policies/data-protection/data-protection-regulation/

Check Point (2022). *What is a Cyber Attack*. Dostupné 28. 11. 2022 z https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

Imperva (2023). *What is APT (Advanced Persistent Threat). APT Security.* Dostupné 21. 2. 2023 z https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

Internetem bezpečně (2022a). *Phishing*. Dostupné 30. 11. 2022 z https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/

Internetem bezpečně (2022b). *Ransomware*. Dostupné 30. 11. 2022 z https://www.internetembezpecne.cz/internetem-bezpecne/malware/ransomware/

Interní materiály společnosti RENOMIA

Kohout, R. (2018). *Jak poznat falešný email*. Internetem bezpečně. Dostupné 1. 3. 2023 z https://www.internetembezpecne.cz/jak-poznat-falesny-email/

Krausová, L. (2019). *Láska přes internet může vyjít pěkně draze*. Policie České republiky. Dostupné 18. 11. 2022 z https://www.policie.cz/clanek/laska-pres-internet-muze-vyjit-pekne-draze.aspx

Lye, J. (2022). *What is review bombing—and why does it need to stop*. VOGUE. Dostupné 27. 2. 2023 z https://vogue.sg/review-bombing-opinion/

Matějíček, P. (2021). *Blagging - podvodná žádost o finanční pomoc*. Spajk.cz. Dostupné 27. 2. 2023 z https://spajk.cz/blagging-podvodna-zadost-o-financni-pomoc/

Ministerstvo financí České republiky (2014a). *Obecně | Pojištění | Proč se finančně vzdělávat. https://financnigramotnost.mfcr.cz/cs/pojisteni/pojisteni-obecne*

Ministerstvo financí České republiky (2014b). *Život a zdraví | Pojištění | Proč se finančně vzdělávat? https://financnigramotnost.mfcr.cz/cs/pojisteni/zivot-a-zdravi*

Ministerstvo vnitra České republiky (2022). *Bezpečnostní hrozby*. Dostupné 10. 11. 2022 z https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

Ministerstvo vnitra České republiky (2023). *Co je GDPR - Ochrana osobních údajů*. Dostupné 1. 3. 2023 z https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

MONETA Money bank (2022a.). *Pojištění*. https://www.moneta.cz/slovnik-pojmu/detail/co-je-pojisteni

MONETA Money bank (2022b). Rizikové pojištění. https://www.moneta.cz/slovnik-pojmu/detail/co-je-rizikove-pojisteni

Morris, R. (2021). *History of cyber insurance*. Marsh Commercial. Dostupné 4. 3. 2023 z https://www.marshcommercial.co.uk/articles/history-of-cyber-insurance/

Northbridge Insurance (2022). *What is cyber risk, and why should I care*. Dostupné 15. 11. 2022 z https://www.northbridgeinsurance.ca/blog/what-is-cyber-risk-2/

NÚKIB (2023). *Legislativa.* Dostupné 25. 2. 2023 z https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

Policie České republiky (2022). Kyberkriminalita. Dostupné 18. 11. 2022 z https://www.policie.cz/clanek/kyberkriminalita.aspx

Policie České republiky (2023). *Jednotlivé druhy kyberkriminality*. Dostupné 27. 2. 2023 z https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

RENOMIA (2023a). *Máte obavu z kybernetických útoků na vaši firmu? Jedním z účinných opatření*. Dostupné 21. 2. 2023 z https://www.renomia.cz/blog/mate-obavu-z kybernetickych-utoku-na-vasi-firmu-jednim-z-ucinnych-opatreni-je-po

RENOMIA (2023b). *Cyber, pojištění kybernetických rizik*. Dostupné 25. 2. 2023 z https://www.renomia.cz/cyber

Sheth, S. N. (2020). *GRC 101: Definition, Examples, and How to Manage Cyber Risk*. LogicGate. Dostupné 9. 11. 2022 z https://www.logicgate.com/blog/grc-101-what-is-cyber-risk/

Schäferhoff, N. (2022). *Co je DDoS útok – a jak mu můžete zabránit*? Raidboxes. Dostupné 20. 2. 2023 z https://raidboxes.io/cs/blog/security/ddos-attack/

Všeobecné a zvláštní pojistné podmínky jednotlivých pojišťoven

Zákony pro lidi (2022). *277/2009 Sb. Zákon o pojišťovnictví*. https://www.zakonyprolidi.cz/cs/2009-277

Zpráva o stavu kybernetické bezpečnosti za rok 2020, NÚKIB

Zpráva o stavu kybernetické bezpečnosti za rok 2021, NÚKIB

Seznam tabulek

Seznam obrázků

Seznam zkratek

APT	Advanced Persistent Threat
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
GDPR	General Data Protection Regulation
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PIN	Personal Identification Number
PR	Public Relations
USA	Spojené státy Americké
VPP	Všeobecné pojistné podmínky
ZPP	Zvláštní pojistné podmínky

Přílohy

Seznam příloh

Příloha I: Dotazník

Příloha II: Cyber dotazník

Příloha I: Dotazník

1. Kolik Vám je let?
Nápověda k otázce: Vyberte jednu odpověď

- Méně než 20 let
- 20 - 30 let
- 31 - 40 let
- 41 - 60 let
- 61 let a více

2. Jaké je Vaše nejvyšší dosažené vzdělání?
Nápověda k otázce: Vyberte jednu odpověď

- Základní
- Středoškolské bez maturity
- Středoškolské s maturitou
- Vyšší odborné
- Vysokoškolské

3. V jakém oboru je Vaše nejvyšší dosažené vzdělání?

4. Jak podle Vás vypadá dostatečně silné heslo?
Nápověda k otázce: Vyberte jednu odpověď

- hesloheslo
- 123456789
- 1111111111
- Ko1Le2Di3Pe4Ok5!
- michalnovak

5. Je tato e-mailová adresa bezpečná a důvěryhodná?
ceskasporitelna@alliance.forspi.com
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

6. Zadali byste přihlašovací údaje k internetovému bankovnictví do odkazu, který by přišel z výše uvedené e-mailové adresy?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

7. Máte ve všech Vašich zařízení (mobilní telefon, tablet, počítač) nainstalované aktuální antivirové programy?
Nápověda k otázce: Vyberte jednu odpověď

- Ano, ve všech
- Ne, nemám
- Pouze v některých

8. Zálohujete pravidelně svá data? (1x za měsíc)
Nápověda k otázce: Vyberte jednu odpověď

- Ano, pravidelně
- Ne, nezálohuji
- Ano, nepravidelně

9. Sdělil/a jste někomu své přihlašovací údaje k internetovému bankovnictví nebo PIN karty?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

10. Ukládáte si přihlašovací údaje do internetových prohlížečů?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

11. Používáte k placení mobilní telefon?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

12. Jaké ověření používáte při placení mobilním telefonem?
Nápověda k otázce: Vyberte jednu nebo více odpovědí

- Otisk prstu
- PIN kód
- Scan obličeje
- Znak
- Heslo
- Žádné
- Jiná

13. Byl/a jste někdy terčem kybernetického útoku?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

14. Jste pojištěný/á proti kybernetickému riziku?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

15. Uvažujete o tom, že se necháte proti kybernetickému riziku pojistit?
Nápověda k otázce: Vyberte jednu odpověď

- Ano
- Ne

Příloha II: Cyber dotazník

Dotazník pro pojištění kybernetických rizik
Questionnaire for Cyber Risks Insurance

Tento dotazník je shrnutím informací potřebných k vypracování návrhu pojištění. Uveďte prosím požadované informace, které se týkají Vaší společnosti, a veškeré další informace, které považujete v této souvislosti za důležité. V případě potřeby uvádějte informace na samostatný list. Informace uvedené v dotazníku jsou důvěrné a budou použity pouze pro potřebu pojištění. Neúplnost nebo nesprávnost sdělených informací mohou ovlivnit naše doporučení týkající se pojištění a samotnou kvalitu pojištění. Děkujeme Vám za spolupráci.

This questionnaire is a summary of the information necessary for preparing an offer of insurance. Please provide the required information that relates to your company, plus all other information that you consider to be important with regard to this insurance. If necessary, provide the information on separate sheets of paper. The information within this questionnaire is of a confidential nature and shall be used only as required for this insurance. Any incomplete or incorrect information may affect our recommendations and suitability of the insurance. Thank you for your cooperation.

1. Všeobecné informace o společnosti/pojistníkovi
General information about the company / Policyholder

Obchodní jméno společnosti: / Company business name:

Sídlo: / Registered office / address:

Hlavní předmět činnosti: / Main business activity:

IČ/DIČ: / Reg. No. / VAT No.:

Webová stránka (včetně dceřiných spol.): / Web page (including subsidiaries):

Počet klientů / fyzických osob, jejichž osobní údaje jsou shromažďovány (odhad): / Number of clients / individuals whose personal data is collected (estimate):

Počet klientů / právnických osob (odhad): / Number of clients / legal entities (estimate):

Počet zaměstnanců: / Number of employees:

2. Dceřiné společnosti
Subsidiaries

Požadujete, aby pojistné krytí zahrnovalo rovněž Vaše dceřiné společnosti? Pokud ano, pak uveďte níže jejich název, IČ, sídlo a předmět činnosti. Do you require the insurance cover to include your subsidiaries as well? If yes, please state below the name, registration no., registered office / address and business activity of the subsidiaries.	☐ Ano Yes ☐ Ne No

V případě, že požadujete, aby se pojistné krytí vztahovalo rovněž na Vaše dceřiné společnosti, odpovídejte prosím na všechny níže/dále uvedené otázky i za všechny takové osoby.
Where insurance cover is also required for subsidiaries, please answer all the questions below in respect of such subsidiaries.

Má Vaše společnost aktiva nebo dceřinou společnost v USA? Does your company have assets or subsidiary in the USA?	☐ Ano Yes ☐ Ne No

3. Finanční údaje (v případě pojištění rovněž dceřiných firem čísla konsolidovaná):
Financial data (consolidated figures in the case of insurance of subsidiaries):

Uveďte celkové roční příjmy (včetně online prodejů) rozdělené dle zemí klientů:
Please provide the total annual turnover (including online sales) split by client location:

	Minulý rok / Last year	Odhad aktuální rok / Current year estimate
Celkové roční příjmy (v Kč) / Total annual turnover (in CZK)		
ČR / Czech Republic		
Země Evropské unie / EU countries		
USA/Kanada / USA / Canada		
Ostatní země / Other countries		

Uveďte celkové roční příjmy jen z online prodejů rozdělené dle zemí klientů:
Please provide the total annual turnover only from online sales split by client location:

	Minulý rok / Last year	Odhad aktuální rok / Current year estimate
Celkové roční příjmy (v Kč) / Total annual turnover (in CZK)		
ČR / Czech Republic		
Země Evropské unie / EU countries		
USA/Kanada / USA / Canada		
Ostatní země / Other countries		

4. Požadovaný rozsah pojistné ochrany
Requested scope of the insurance cover

Uveďte požadované limity pojistného plnění a spoluúčasti:
Please state the required limits of indemnity and deductible:

a) Limity pojistného plnění, pro něž požadujete nabídku (varianty): / Limits of indemnity you require (options):
b) Spoluúčast (varianty): / Deductible (options):
c) Počátek pojištění: / Insurance inception date:

Základní rozsah pojistného krytí: Odpovědnost za data a zabezpečení sítě + Regulatorní řízení včetně pokut + Náklady pojištěného na odborné služby (IT, PR, oznámení, obnova dat)
Basic scope of insurance cover: Data Liability and Network Security plus Administrative Obligations, including fines and Insured's costs for professional services (IT, PR, notification, and data recovery)

Požadovaný nadstandardní rozsah pojištění:
Required above standard scope of cover:

- ☐ Vydírání prostřednictvím sítě („ransomware") / Cyber extortion ("ransomware")
- ☐ Zveřejnění digitálního obsahu v multimédiích / Odpovědnost v souvislosti s médii
  Publishing of digital content in multimedia / media liability
- ☐ Výpadek sítě (přerušení provozu) / Network interruption (business interruption)
- ☐ Kybernetické trestné činy / Cyber Crime

5. Stávající/předchozí pojištění
Current / previous insurance

5.1 Máte v současnosti nebo jste v minulosti měli pojištění kybernetických rizik, které poskytovalo stejné nebo podobné krytí jako pojištění, o které máte zájem? Do you currently have or have you ever had any cyber risks insurance providing the same or similar coverage as the insurance you are interested in?	☐ Ano / Yes ☐ Ne / No
5.2 Došlo někdy ze strany pojistitele k zamítnutí předložení nabídky nebo ke zrušení nebo neobnovení pojištění, která poskytovala stejné nebo podobné krytí jako pojištění, o které žádáte? Has any insurer ever refused to provide an offer, or cancelled or not renewed a policy that provided the same or similar coverage as the insurance you are asking for?	☐ Ano / Yes ☐ Ne / No

6. Postupy při ochraně údajů
Data protection procedures

6.1 Podléhá Vaše společnost pravidlům Evropské unie pro nakládání a zpracování osobních údajů? Pokud „Ne“, uveďte prosím zemi/země, jejichž pravidlům podléháte. Is your company subject to European Union rules on the handling and processing of personal data? If "No", please indicate the country whose rules you are subject to. Země: / Country:	☐ Ano / Yes ☐ Ne / No
6.2 Provedla Vaše společnost revizi postupů ve vztahu ke zpracování údajů a zjistila oblasti, které mohou způsobit problémy s dodržováním postupů dle GDPR a přijala nebo přijímá přiměřená technická a organizační opatření k tomu, aby byla v souladu s GDPR řádně dokumentovaným způsobem? Has your company reviewed the processes related to data protection and identified any potential compliance issues under the General Data Protection Requirements (GDPR) and implemented reasonable technical and organizational measures to make the organisation compliant with GDPR in a formally documented way?	☐ Ano / Yes ☐ Ne / No
6.3 Je Vaše společnost povinna jmenovat osobu odpovědnou za ochranu osobních údajů („DPO“)? Pokud „Ano“, uveďte prosím identifikační údaje takové odpovědné osoby: Is your company obliged to appoint a data protection officer ("DPO")? If "Yes", please provide identification data for the person responsible. Pokud „Ne“, kdo odpovídá za bezpečnost osobních údajů a jiných údajů a za dodržování legislativy? If "No", who is responsible for the safety of personal data and other data and compliance with legislation?	☐ Ano / Yes ☐ Ne / No

6.4 Existuje písemná směrnice (či jiný obdobný dokument), podle které postupujete ve vztahu k Vámi zpracovávaným osobním údajům a jiným datům? Pokud „Ano", byla taková směrnice revidována právním zástupcem a kdy? Are there written guidelines (or other similar documents) under which you proceed in relation to processing of personal data and other data? If "Yes", were such guidelines reviewed by a lawyer and when? Pokud „Ne", uveďte prosím, jakým způsobem zajišťujete ochranu osobních údajů a jiných dat: If "No", please specify the way you ensure the protection of personal data and other data:	☐ Ano Yes ☐ Ne No
6.5 Jsou všichni zaměstnanci Vaší společnosti s touto směrnicí prokazatelně obeznámeni a absolvují pravidelná školení v oblasti ochrany osobních údajů? Are all your employees demonstrably familiar with these guidelines and do they attend regular training with respect to personal data protection? Pokud „Ne", uveďte důvody a způsob, jak jinak tuto oblast řešíte: If "No", please provide reasons and how this area is addressed	☐ Ano Yes ☐ Ne No
6.6 Je uvedená směrnice a/nebo postupy společnosti v oblasti ochrany osobních údajů a jiných dat v souladu s příslušnými právními předpisy právních řádů všech zemí, ve kterých podnikáte a máte klienty? Are these guidelines and/or company's procedures for personal data and other data protection in accordance with the applicable laws of all the countries where you do business and where you have clients? Pokud „Ne", uveďte prosím, se kterými právními řády není v souladu, a důvod: If "No", please state with which law is inconsistent and why?	☐ Ano Yes ☐ Ne No
6.7 Má Vaše společnost interně řešeno podávání oznámení subjektu osobních údajů ohledně incidentů ve spojitosti s bezpečností osobních údajů? Within your company, do you have a system how to inform individuals about incidents connected with breaching of their personal data?	☐ Ano Yes ☐ Ne No
6.8 Má Vaše společnost interně řešeno podávání oznámení příslušnému úřadu pro ochranu osobních údajů ohledně incidentů ve spojitosti s bezpečností osobních údajů? Within your company, do you have a system how to report incidents to the relevant office dealing with breaching of personal data security?	☐ Ano Yes ☐ Ne No
6.9 Přijala Vaše společnost interní postup pro zajištění pravidelné (nejméně každoroční) revize a v případě potřeby i aktualizace Oznámení týkajících se ochrany dat a Souhlasů? Has your company adopted internal procedures to ensure a regular (at least yearly) review and, if needed, to update the data protection notice and consents?	☐ Ano Yes ☐ Ne No
6.10 Zajišťuje Vaše společnost bezpečné nakládání s dokumenty obsahujícími citlivé údaje (např. jejich ukládání do zamykatelných skříní)? Does your company ensure that paper documents containing sensitive information are secured at all times (e.g. locked filling cabinets)?	☐ Ano Yes ☐ Ne No
6.11 Jsou osobní data šifrována při uložení do informačních systémů a při přenosu po síti? Are personal data encrypted when stored in information systems and when transmitted over the network?	☐ Ano Yes ☐ Ne No

6.12 Byli všichni zaměstnanci obeznámeni s opatřeními týkajícími se ochrany osobních údajů? Are all employees familiar with personal data protection measures?	☐ Ano Yes ☐ Ne No
6.13 Pokud Vaše společnost vykonává činnosti v sektorech, kde dochází ke zpracování osobních údajů dle zvláštního právního předpisu (např. poskytování zdravotních služeb; poskytování komunikačních a telekomunikačních služeb; dodávky a distribuce elektrické energie, plynu, vody, atd.; poskytování bankovních a platebních služeb; pojišťovací služby, zprostředkování pojišťovacích služeb aj.), monitoruje Vaše společnost dodržování zvláštních zákonných povinností týkajících se ochrany osobních údajů v souladu s příslušnou legislativou? If your company carries out activities in a sector in which personal data is processed under special legal regulations (e.g. provision of healthcare services; provision of communication and telecommunication services; provision of and distributing electricity, gas, water, etc.; provision of banking and payment services; insurance services, insurance intermediary services and others), does your company monitor compliance of such special legal obligations regarding personal data protection pursuant to such special legal regulations?	☐ Ano Yes ☐ Ne No

7. Kvalita a množství dat, ONLINE činnosti a služby
Quality and quantity of data, ONLINE activities and services

Jaký typ údajů Vaše společnost uchovává a zpracovává?
Which type of data is your company maintaining and processing?

- ☐ Osobní údaje / Personally Identifiable Information (PII)
- ☐ Duševní vlastnictví / Intellectual Property (IP)
- ☐ Informace o zdravotním stavu / Personal Health Information (PHI)
- ☐ Informace o platebních kartách / Payment Card Information (PCI)
- ☐ Uživatelská jména a hesla / Usernames and passwords

7.1 Pokud je výše zvolena možnost „Informace o platebních kartách", splňuje Vaše společnost bezpečnostní standard PCI DSS (Payment Card Industry Data Security Standards)? If "Payment Card Information" is selected above, does your company comply with PCI DSS (Payment Card Industry Data Security Standards)?	☐ Ano Yes ☐ Ne No
7.2 Pokud uchováváte výše uvedené citlivé údaje, je přístup k takovým údajům omezený? If you maintain the above sensitive data, is access to such data restricted?	☐ Ano Yes ☐ Ne No
7.3 Kontrolujete/zpracováváte osobní údaje občanů USA? Do you control/process the personal data of US citizens?	☐ Ano Yes ☐ Ne No

Uveďte prosím (odhadovaný) objem citlivých údajů (počet záznamů), který Vaše společnost uchovává/zpracovává.
Please state (estimated) volume of sensitive data (number of unique records) your company is maintaining/processing.

- ☐ méně než 1 000 / less than 1 000
- ☐ 1 000 až 10 000 / 1 000 to 10 000
- ☐ 10 000 až 100 000 / 10 000 to 100 000
- ☐ více než 100 000 / more than 100 000

8. Odpovědnost v souvislosti s médii
Media liability coverage

Prosím odpovězte na následující otázky, pokud žádáte o (volitelné) krytí Zveřejnění digitálního obsahu v multimédiích / Odpovědnost v souvislosti s médii. Jaký druh elektronických/online činností společnost provozuje? Prosím zaškrtněte vše, co se hodí.
Please answer the following questions if you are applying for the (optional) liability cover for Publishing of digital content in multimedia / media. What kind of electronic / online activities does the company perform? Please check all that apply.

- ☐ Publikování vlastního elektronického obsahu / Electronic own content publishing
- ☐ Streaming video nebo hudebního obsahu na základě písemných licenčních smluv/souhlasů / Streaming video or music content under written licenses / content agreements
- ☐ Sběr citlivých údajů / Collection of sensitive information
- ☐ Poskytování poradenství (např. zdravotnictví, právní apod.) / Giving advice (e.g. medical, legal etc.)
- ☐ Obsah na základě licence od třetí strany / Content under license from a third party
- ☐ Prezentace produktů/služeb druhých (reklama, nákup nebo prodej) / Presentation of products / services of others (advertising, buying or selling)
- ☐ Nelicencovaný obsah třetích stran (např. chatovací místnosti, blogy, nástěnky, zákaznické recenze) / Unlicensed third party content (e.g. chat rooms, blogs, message boards, customer reviews)
- ☐ Soubory ke stažení / Files for download

Poskytuje web Vaší společnosti ochranu soukromí (např. ohledně sběru dat, používání cookies atd.) a uvádí zákonné oznámení o užívání práv třetích stran a odkazy na externí stránky, včetně prohlášení o zřeknutí se odpovědnosti (tzv. „Disclaimer"), a je takový obsah schválen kvalifikovaným právním poradcem? Does your company's website provide a privacy policy (e.g. about data collection, use of cookies etc.) and a legal notice about use of third parties' rights and links to external websites including a Disclaimer, and is such content approved by a competent legal counsel?	☐ Ano / Yes ☐ Ne / No

9. Služby třetích stran (subdodavatelé)
Third party services (subcontractors)

Využívá Vaše společnost subdodavatelů na jakoukoli část sítě, počítačového systému nebo funkci na zabezpečení údajů? Zaškrtněte vše, co se hodí, a uveďte organizaci poskytující služby:
Does your company outsource any part of your network, computer system or information security functions? Check all that apply and name the organization providing the services:

- ☐ Řízení celého IT systému / Management of entire IT system
- ☐ Zpracovávání dat / Data processing
- ☐ Poskytovatel aplikační služby / Application service provider
- ☐ Offsite zálohování a uchovávání / Offsite backup and storage
- ☐ Jiné cloudové výpočetní služby / Other cloud computing services

9.1 Máte podepsanou písemnou smlouvu s příslušnými poskytovateli služeb, včetně dohody o mlčenlivosti, a provádí společnost pravidelně audit funkcí subdodavatele, aby zajistila, že se řídí bezpečnostními předpisy společnosti? Zaškrtněte N/A (nehodí se), jen pokud nemáte subdodavatele na žádnou část své sítě, počítačového systému nebo funkcí zabezpečení informací. Do you have a written and signed contract with the respective service provider(s) including a non-disclosure / confidentiality agreement, and does the company periodically audit the functions of subcontractors to ensure that they follow the company's security policies? Check N/A only if you do not outsource any part of your network, computer system or information security functions.	☐ Ano / Yes ☐ Ne / No ☐ Nehodí se / N/A
9.2 Vzdali jste se svých práv na náhradu škody vůči poskytovateli služeb ve smlouvě o outsourcingu? Have you waived your rights to damages in relation to the service provider in the outsourcing contract?	☐ Ano / Yes ☐ Ne / No
9.3 Požaduje Vaše společnost, aby organizace poskytující sběr dat nebo zpracovávání údajů (subdodavatelé) udržovaly také své pojištění odpovědnosti ve vztahu k ochraně údajů (pojištění profesní odpovědnosti)? Does your company require that data collection or data processing organisations (subcontractors) also maintain their data protection liability insurance (professional liability insurance)?	☐ Ano / Yes ☐ Ne / No

10. IT bezpečnost – ochrana organizace
IT security – organisational protection

10.1 Má Vaše společnost odpovědnou osobu nebo tým v oblasti IT bezpečnosti, který pravidelně podává hlášení managementu? Does the company have an individual or team that is responsible for IT security that regularly reports to management?	☐ Ano / Yes ☐ Ne / No
10.2 Je společnost držitelem platného certifikátu nebo byla úspěšně auditována pro oblast bezpečnosti informací, např. ISO 27001 apod.? Pokud ano, uveďte prosím v dalším řádku specifikaci. Does the company hold a valid certificate or has it been successfully audited for information security, e.g. ISO 27001, etc.? If so, please provide specifications in the following row.	☐ Ano / Yes ☐ Ne / No
10.3 Školíte pravidelně své zaměstnance v oblasti IT bezpečnosti? Do you provide regular training for your employees in the area of IT security?	☐ Ano / Yes ☐ Ne / No
10.4 Přistupují interní uživatelé k internetovým stránkám přes síťové zařízení (proxy) vybavené antivirem a filtrem internetového obsahu? Do internal users access websites through a network device (proxy) equipped with an antivirus and an internet content filter?	☐ Ano / Yes ☐ Ne / No
10.5 Máte normu pro vytváření hesel a jsou prosazovány, např. co se týče složitosti (silná hesla), pravidelné změny? Do you have a password policy and is it enforced, e.g. by complexity (strong passwords) and a requirement to regularly change passwords?	☐ Ano / Yes ☐ Ne / No

10.6 Jsou přihlašovací hesla do sítě v délce minimálně 8 znaků v kombinaci velkých, malých písmen a čísel? Are network login passwords at least 8 characters long in a combination of uppercase letters, lowercase letters and numbers?	☐ Ano / Yes ☐ Ne / No
10.7 Jak často musí dojít ke změně hesla? How often do passwords have to be changed?	☐ max. po 3 měsících / less than 3 months ☐ déle než po 3 měsících / more than 3 months
10.8 Má Vaše společnost zaveden plán zachování provozu (BCP – „Business continuity plan") pro riziko kybernetického ohrožení, který je pravidelně testován a aktualizován? Does your company have a Business Continuity Plan (BCP) in place for cyber threat risk which is regularly tested and updated?	☐ Ano / Yes ☐ Ne / No

Maximální doba výpadku IT systému než dojde k závažnému dopadu na Vaši činnost.
Maximum outage period from business interruption of an IT system before there is a significant adverse impact on your business:

- ☐ méně než 12 hodin / less than 12 hours
- ☐ 12–24 hodin / 12–24 hours
- ☐ 24–48 hodin / 24–48 hours
- ☐ více než 48 hodin / more than 48 hours

10.9 Jsou penetrační testy prováděny pravidelně a v případě potřeby je implementován plán nápravy? Are penetration tests performed regularly and is a remediation plan implemented if necessary?	☐ Ano / Yes ☐ Ne / No
10.10 Má Vaše společnost zavedenu koncepci dispečerského řízení a sběru dat (tzv. SCADA – „Supervisory control and data acquisition") pro klíčovou infrastrukturu a výrobní/provozní technologické procesy? Does your company have a SCADA ("Supervisory Control and Data Acquisition") concept implemented for its key infrastructure and manufacturing/operational technology processes?	☐ Ano / Yes ☐ Ne / No ☐ Nehodí se / N/A

11. IT bezpečnost – technická ochrana
IT security – technical protection

11.1 Používáte antivirus, anti-spyware nebo ekvivalentní ochranu proti malwaru? Do you use anti-virus, anti-spyware or equivalent malware protection?	☐ Ano / Yes ☐ Ne / No
11.2 Pokud ano, jsou Vaše antivirové programy stahovány a aktualizovány automaticky? If yes, is your anti-virus software downloaded and updated automatically?	☐ Ano / Yes ☐ Ne / No
11.3 Používáte aktuální software podporovaný ze strany výrobce? Do you use updated software supported by the manufacturer?	☐ Ano / Yes ☐ Ne / No
11.4 Jsou pravidelně nasazovány bezpečnostní softwarové aktualizace? Do you perform regular security software updates?	☐ Ano / Yes ☐ Ne / No
11.5 Provádíte pravidelnou kontrolu informačních systémů a implementujete vyplývající doporučení? Do you perform regular checks of information systems and do you implement the resulting recommendations?	☐ Ano / Yes ☐ Ne / No

11.6 Identifikujete kritická rizika informačních systémů a podnikáte vhodné kroky k jejich zmírnění? Do you identify critical risks to information systems and do you take appropriate steps to mitigate them?	☐ Ano / Yes ☐ Ne / No
11.7 Vyžaduje přístup do kritických informačních systémů dvojí ověření? Does access to critical information systems require double authentication?	☐ Ano / Yes ☐ Ne / No
11.8 Máte zajištěno, aby všechna výchozí hesla na všech počítačových systémech (např. router) byla pravidelně měněna? Is it ensured that all default passwords on all computer systems (e.g. router) are changed regularly?	☐ Ano / Yes ☐ Ne / No
11.9 Monitoruje společnost své sítě a počítačové systémy na narušení datové bezpečnosti? Does the company monitor its networks and computer systems for breaches of Data Security?	☐ Ano / Yes ☐ Ne / No
11.10 Jsou mobilní zařízení (laptopy, chytré telefony, USB zařízení, pevné disky notebooků atd.) chráněny heslem? Are mobile devices (laptops, smartphones, USB devices, etc.) and laptop hard drives password protected?	☐ Ano / Yes ☐ Ne / No
11.11 Je síť segmentována za účelem oddělení kritických oblastí od nekritických? Is the network segmented to separate critical areas from non-critical areas?	☐ Ano / Yes ☐ Ne / No
11.12 Má Vaše společnost zavedeny fyzické kontroly, aby zabránila neautorizovanému přístupu ke svému počítačovému systému a datacentru a mohla by takový přístup detekovat? Does your company have physical security controls in place to prohibit and detect unauthorized access to its computer system and data centre?	☐ Ano / Yes ☐ Ne / No

11.13 Má datové centrum hostující kritické systémy odolnou infrastrukturu včetně záložní (náhradní) dodávky energie a síťového připojení? Does the data centre hosting critical systems have a resilient infrastructure, including backup (replacement) power supply and network connectivity?	☐ Ano / Yes ☐ Ne / No
11.14 Probíhá zálohování dat denně, zálohy jsou pravidelně testovány a jejich kopie pravidelně umisťovány na vzdáleném místě? Is data backed up daily, are backups tested regularly, and are their copies regularly placed at a remote location?	☐ Ano / Yes ☐ Ne / No
11.15 Vyžaduje Vaše společnost, aby vzdálení uživatelé byli ověřeni, než se mohou připojit k interním sítím a počítačovým systémům? Does your company require remote users to be authenticated before being allowed to connect to internal networks and computer systems?	☐ Ano / Yes ☐ Ne / No
11.16 Pokud ano, jak často? If yes, how often?	☐ 1x denně / once a day ☐ 1x týdně / once a week
11.17 Zajišťujete pravidelně, aby datové zálohy bylo možné obnovit co nejrychleji a s minimálním dopadem? Do you regularly ensure that data backups can be restored as quickly as possible and with minimal impact?	☐ Ano / Yes ☐ Ne / No

Pokud „Ano", jakou dobu potřebujete na plné obnovení klíčových IT systémů a dat?
If "yes", what is the period needed to fully restore key IT systems and data?

- ☐ méně než 8 hodin / less than 8 hours
- ☐ 8–24 hodin / 8–24 hours
- ☐ 24–48 hodin / 24–48 hours
- ☐ více než 48 hodin / more than 48 hours

12. Bezpečnostní IT incidenty a historie ztrát
IT security incidents and loss history

Došlo ve Vaší společnosti v posledních pěti letech k narušení IT bezpečnosti, poškození sítě, systému nebo ztrátě dat? Within the last five years, has your company suffered any violation of IT security, network/ system damage or loss of data?	☐ Ano Yes ☐ Ne No

Pokud „ Ano", jaká byla finanční ztráta Vaší společnosti v důsledku této události?
If "yes", what was the financial loss your company suffered as a result of such events?

☐ <1 mil. Kč / <CZK 1m ☐ 1 mil. Kč – 5 mil. Kč / CZK 1m – CZK 5m ☐ > 5 mil. Kč / > CZK 5m

Došlo v posledních 12 měsících k výpadku funkčnosti počítačů, systémů nebo IT služeb, který trval déle než 4 hodiny? Has there been a malfunction of computers, systems or IT services in the last 12 months lasting more than 4 hours?	☐ Ano Yes ☐ Ne No
Došlo v posledních třech letech k oznámení ze strany Vašeho zákazníka, že jeho údaje byly zneužity? Within the last three years, has any customer claimed that its data has been compromised?	☐ Ano Yes ☐ Ne No

Pokud „ Ano", jaká byla finanční ztráta Vaší společnosti v důsledku této události?
If "yes", what was the financial loss your company suffered as a result of this event?

☐ <1 mil. Kč / <CZK 1m ☐ 1 mil. Kč – 5 mil. Kč / CZK 1m – CZK 5m ☐ > 5 mil. Kč / > CZK 5m

Byla Vaše společnost vyšetřována nebo podrobena auditu ve vztahu k ochraně osobních údajů ze strany Úřadu pro ochranu osobních údajů nebo jiného dozorového orgánu? Has your company been the subject of any investigation or audit in relation to personal data protection by a data protection authority or other supervisory authority?	☐ Ano Yes ☐ Ne No
Jste si Vy nebo jiný spolupojištěný vědomi okolností, které by mohly vést k nároku na plnění v souvislosti s tímto pojištěním? Are you or any co-insured aware of circumstances that could lead to a claim under this insurance?	☐ Ano Yes ☐ Ne No

Pokud jste v kterémkoli z výše uvedených případů zaškrtli „ Ano", uveďte prosím detail:
If you checked "Yes" for any of the above, please provide details:

Společnost RENOMIA Vám děkuje za vyplnění tohoto dotazníku.
RENOMIA thanks you for completion of this questionnaire.

Datum: / Date:

Vyplnil: / Completed by:

Razítko a podpis: / Stamp and signature:

Prohlašujeme tímto, že všechny informace uvedené v tomto dokumentu jsou úplné, pravdivé a přesné a taktéž, že informace nám byly poskytnuty srozumitelně, jasně a přesně. Zavazujeme se, že budeme informovat zprostředkovatele pojištění a pojistitele o podstatných změnách ohledně zaznamenaných skutečností, ke kterým by došlo před uzavřením nebo po uzavření pojistné smlouvy. Zároveň souhlasíme s tím, aby informace sdělené v tomto dokumentu byly použity pro účely předsmluvní dokumentace a informační povinnosti zprostředkovatele a pojistitele. Tento dokument obsahuje informace důvěrného charakteru. Žádná část dokumentu nesmí být kopírována, uveřejněna či jinak poskytnuta třetí straně bez předchozího písemného souhlasu RENOMIA, a. s. Dotazník vyplnila osoba oprávněná jednat jménem společnosti.

Pokud máte nějaké komentáře k jakékoliv otázce, uveďte zde prosím její číslo a doplňující text.
If you have any comments on any question, please provide its number and additional text here.

Abstrakt

Pacáková, T. (2023). *Pojištění kybernetických rizik* [Diplomová práce, Západočeská univerzita v Plzni].

Klíčová slova: kybernetický útok, kybernetické riziko, pojištění kybernetických rizik

Diplomová práce se zabývá problematikou pojištění kybernetických rizik. Teoretická část se nejprve zaměřuje na definici pojištění. Následně jsou kybernetické útoky rozděleny podle toho, zda jsou cílené na jednotlivce nebo na společnosti. Dále je představena stručná historie pojištění kybernetických rizik a legislativa, která toto pojištění upravuje. Praktická část diplomové práce se zabývala analýzou a komparací produktové nabídky vybraných komerčních pojišťoven. Součástí praktické části je dotazníkové šetření, které zkoumá chování obyvatel České republiky v oblasti kybernetických rizik. Výstupem práce je zhodnocení produktové nabídky pojišťoven a dále objasnění chovaní obyvatel České republiky v oblasti kybernetických rizik.

Abstract

Pacáková, T. (2023). *Cyber risk insurance* [Master's Thesis, University of West Bohemia].

Key words: cyber attack, cyber risk, cyber risk insurance

Diploma thesis deal with the issue of cyber risk insurance. In the theoretic section there is a definition of insurance. After that cyber attacks are divided into companies and individuals based on who they are targeting. Next chapter is about history of cyber risk insurance and about legislation. The practical section of the diploma thesis includes analysis and comparison of the product offer of insurance companies. Also, in the practical section there is a survey. The survey is about behavior of people from the Czech Republic in the area of cyber risk. The result of the diploma thesis is evaluation of the product offer of insurance companies. And also clarify behavior of people from the Czech Republic in the area of cyber risk.